2014

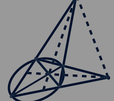


Introducción a la Teoría de números

Primera edición

Walter Mora F.

2014



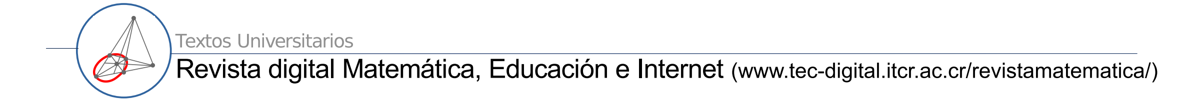
Revista digital Matemática, Educación e Internet

https://tecdigital.tec.ac.cr/revistamatematica/

INTRODUCCIÓN a la TEORÍA DE NÚMEROS.

Ejemplos y algoritmos.

Prof. Walter Mora F.,
Escuela de Matemática
Instituto Tecnológico de Costa Rica.
(https://tecdigital.tec.ac.cr/revistamatematica/)



Correo Electrónico: wmora2@gmail.com
Escuela de Matemática
Instituto Tecnológico de Costa Rica
Apdo. 159-7050, Cartago
Teléfono (506)25502225
Fax (506)25502493

Mora Flores, Walter.
Introducción a la Teoría de Números. Ejemplos y algoritmos. 1ra ed.
– Escuela de Matemática,Instituto Tecnológico de Costa Rica. 2010.
219 pp.
ISBN Obra Independiente: 978-9968-641-11-1
1. Teoría de números. 2. Algoritmos 3. Programación.

Contenido

Prefacio

La Teoría de Números estudia los números enteros y, en cierta medida los números racionales y los números algebraicos. La Teoría Computacional de Números (Computational Number Theory) es sinónimo de Teoría Algorítmica de Números. Aquí se estudia los algoritmos eficientes para cálculos en teoría de números. Este es un libro introductorio orientado hacia la teoría algorítmica de números. El interés es mostrar el valor puramente teórico de algunos teoremas y cómo se debe hacer una variación si el propósito es cálculos rápidos y eficientes. Algunas algoritmos sencillos se implementan en VBA Excel o en LibreOffice Basic por ser lenguajes muy amigables y por ser las hojas electrónicas muy familiares para los estudiantes. Sin emabargo estas implementaciones son muy límitadas y solo tienen fines didácticos. Otras implementaciones se hacen en Java (para usar enteros y racionales grandes). En el capítulo final se desarrollan algunos programas en Java que sirven de base para implementar otros algoritmos.

Agradezco a las personas que ayudaron con sus comentarios para corregir errores en el texto y los programas y para mejorar algunos párrafos un tanto oscuros. Las actualizaciones del libro (correcciones, nuevos programas, etc.,) estarán en https://tecdigital.tec.ac.cr/revistamatematica//Libros/. También puede solicitar un 'machote' LaTeX del libro.

W. Mora.

Cartago, Costa Rica

Diciembre, 2014.

Parte I

INTRODUCCCION A LA TEORIA DE NUMEROS.

1 FUNDAMENTOS

1.1 Principios

Los números enteros son el ingrediente principal en teoría de números. En esta sección, establecemos brevemente la notación y el significado de algunos símbolos que se relacionan con los enteros y que serán de amplio uso en el texto. Además se establecen algunos principios que se usan ampliamente en los argumentos.

En lo que sigue, usaremos la siguiente notación

a.) $\mathbb{N} = \{0,1,2,...\}$ y $\mathbb{N}^+ = \{1,2,...\}$.

b.) $\mathbb{Z}^+ = \{1,2,...\} = \mathbb{N}^+$

c.) $\mathbb{R}^+ = \{x \in \mathbb{R} \,:\, x > 0\}$.

Principio del Buen Orden: Todo conjunto no vacío de números naturales contiene un elemento mínimo.
En particular, si $S \subset \mathbb{Z}$ y si S tiene al menos un elemento positivo, entonces S tiene un entero positivo mínimo.

Ejemplo 1.1

Probar que si $a,b \in \mathbb{Z}$ con $b \geq 1$, entonces existe $q \in \mathbb{Z}$ tal que $qb \leq a < (q+1)b$.

Solución: Idea: qb sería el múltiplo de b más cercano a a en el sentido de que el siguiente múltiplo, $(q+1)b$, lo sobrepasa; por tanto $a - qb \geq 0$ sería la resta no negativa mínima. La existencia de este elemento mínimo se puede establecer usando el principio del buen orden.

Sea $S = \{a - nb \text{ tal que } n \in \mathbb{Z} \wedge a - nb \geq 0\}$. Primero probamos que S es no vacío. En efecto, Si $a \geq 0$, $a = a - 0 \cdot b \geq 0$, entonces $a \in S$. Si $a < 0$, $a - ab = a(1-b) \geq 0$ pues $b \geq 1$, entonces $a - ab \in S$. Por el principio del buen orden, S tiene un elemento mínimo $a - qb \geq 0$ y, por tanto $a - (q+1)b < 0$. Así, $qb \leq a < (q+1)b$.

Principio del palomar: Si k es un entero positivo y $k+1$ o más objetos son asignados a k cajas, entonces hay al menos alguna caja a la que se le asignaron dos o más objetos.

Ejemplo 1.2

En un grupo de 367 personas, debe haber al menos dos que cumplen años el mismo día, porque hay solo 366 posibles días para cumplir años.

Principio de Inclusión-Exclusión: Sean A y B dos conjuntos finitos. Entonces

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Ejemplo 1.3

Sea $A = \{a,b,c,d\}$ y $B = \{a,b,c,g,h\}$. $|A| = 4$, $|B| = 5$, $|A \cup B| = |\{a,b,c,d,g,h\}| = 6$ y $|A \cap B| = |\{a,b,c\}| = 3$. Luego, $|A \cup B| = 6 = |A| + |B| - |A \cap B| = 4 + 5 - 3$.

Principio de Inducción: Para probar que una proposición $P(n)$ es verdadera para todo entero positivo n, se deben ejecutar los dos pasos siguientes:

a.) Verificar que $P(n)$ se cumple para $n = 1$,

b.) Probar que si se cumple $P(k)$ (hipótesis de inducción), entonces se cumple $P(k+1)$

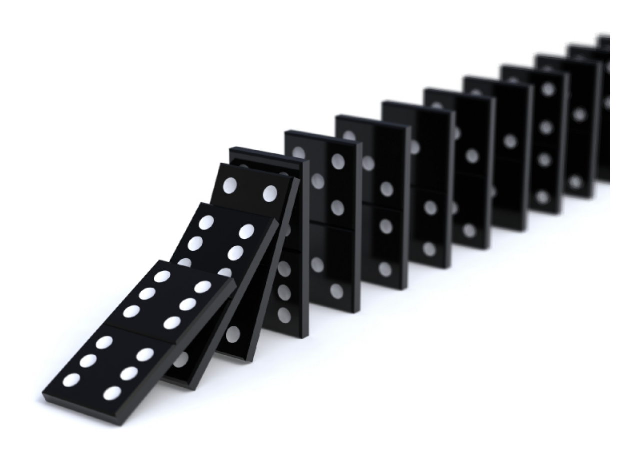


Figura 1.1. Idea de inducción matemática usando un juego de domino.

Se puede probar que el principio de inducción es un método válido de prueba si asumimos el principio del buen orden como un axioma.

Ejemplo 1.4

Históricamente, el primer ejemplo que se conoce en el que se usó inducción matemática aparece en el libro "Arithmeticorum Libri Duo" de Francesco Maurolico (1494-1575). En este libro, entre otras cosas, Maurolico presenta gran variedad de propiedades de los enteros y las pruebas de estas propiedades. Para las demostraciones, él ideo el método de inducción matemática. La primera vez que se usa el método, es para probar que la suma de los primeros n enteros impares es n^2. El nombre "inducción matemática", lo usó por primera vez el matemático inglés John Wallis.

Ex aggregatione imparium numerorum ab vnitate per ordinem successiuè sumptorum, construuntur quadrati numeri continuati ab vnitate, ipsisq; imparibus collaterales. Nam per antepræmissam, vnitas imprimis cum impari sequente facit quadratum sequentem scilicet, 4. Et ipse 4. quadratus secundus, cum impari tertio scilicet 5. facit quadratum tertium, scilicet 9. Itemque 9. quadratus tertius cum impari quarto scilicet 7. facit quadratum quartum, scilicet 16. & sic deinceps in infinitum, semper 13ª repetita propositum demonstratur.

15ª

1, 3 → 4; 5 → 9; 7 → 16; 9 → 25

Figura 1.2. Francesco Maurolico. "Arithmeticorum Libri Duo", pág 7. En `www.books.google.com`

Probar que $1+3+5+...+(2n-1)=n^2$

Solución: En este caso, n indica el número de sumandos.

a.) La proposición es correcta para $n=1$ pues $1=1^2$

b.) Hipótesis de inducción: suponemos que la proposición es cierta para $n=k$, es decir, $1+3+5+...+2k-1=k^2$. Ahora sumamos el siguiente impar, $2k-1\ +2\ =2k+1$, a ambos lados,

$$\overbrace{1+3+5+...+2k-1}^{k^2}\ +\ 2k+1=k^2+2k+1=(k+1)^2.$$

Por lo tanto, hemos demostrado que si la proposición es correcta para $n=k$, es correcta para $n=k+1$. Entonces, la fórmula es válida para todo $n\in\mathbb{N}$, por el principio de inducción.

Principio de Inducción Completa: Para probar que una proposición $P(n)$ es verdadera para todo entero positivo n, se deben ejecutar los dos pasos siguientes:

a.) Verificar que $P(n)$ se cumple para $n=1$,

b.) Probar que si se cumple $P(1)\wedge\ P(2)\wedge\ ...\wedge\ P(k)$ (hipótesis de inducción), entonces se cumple $P(k+1)$

Se puede probar que el principio de inducción completa es equivalente al principio de inducción. Es decir, cada principio puede ser demostrado asumiendo el otro. La ganancia es que el principio de inducción completa es más flexible. A el principio de inducción completa también se le llama "principio de inducción fuerte" o "segundo principio de inducción".

Ejemplo 1.5

Si n es un entero mayor que uno, n se puede escribir como un producto de primos. La demostración de este hecho se hace con inducción fuerte. Puede ver el teorema 2.14, que está más adelante.

1.2 Valor absoluto y la función $\text{sgn}(x)$

Muchas veces es conveniente separar el número y su signo. Para esto usamos la función "*signo*". En las aplicaciones es necesario que esta función solo tome dos valores -1 y 1.

Definición 1.1 (Función signo).
Definimos $\text{sgn}(x) = 1$ si $x \geq 0$ y $\text{sgn}(x) = -1$ si $x < 0$.

Teorema 1.1
Sea $a \in \mathbb{Z}$. Entonces, $|a| = a \cdot \text{sgn}(a) = a/\text{sgn}(a)$.

Ejemplo 1.6

a.) $|-5| = -5 \cdot \text{sgn}(-5) = -5 \cdot -1 = 5$

b.) $|0| = 0/\text{sgn}(0) = 0/1 = 0$

1.3 Las funciones $\lfloor x \rfloor$ $\lceil x \rceil$ y $[\![x]\!]$

Definición 1.2 (Parte entera).

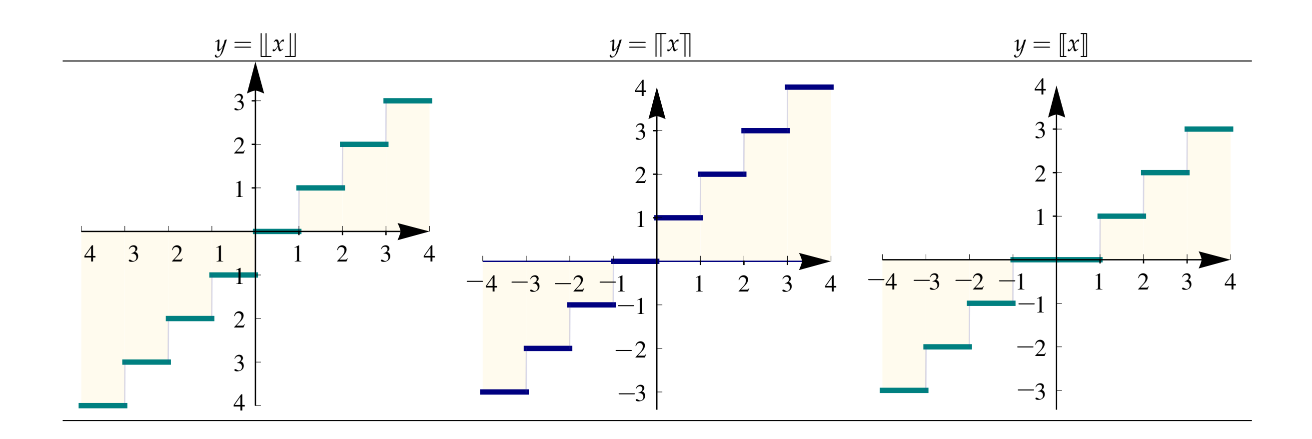
- Función $\lfloor x \rfloor$. Si $x \in \mathbb{R}$ y $n \in \mathbb{Z}$ tal que $n \leq x < n+1$ entonces $\lfloor x \rfloor = n$.
- Función $\lceil x \rceil$. Si $x \in \mathbb{R}$ y $n \in \mathbb{Z}$ tal que $n-1 < x \leq n$ entonces $\lceil x \rceil = n$.
- Función $[\![x]\!]$.

$$[\![x]\!] = \begin{cases} \lfloor x \rfloor & \text{si} \quad x \geq 0 \\ \lceil x \rceil & \text{si} \quad x < 0 \end{cases}$$

Ejemplo 1.7

a.) $\lfloor 1.4 \rfloor = 1$ **b.)** $\lceil 1.4 \rceil = 2$ **c.)** $\lfloor -1.4 \rfloor = -2$ **d.)** $\lceil -1.4 \rceil = -1$ **e.)** $\lceil -3 \rceil = \lfloor -3 \rfloor = -3$.

Representación gráfica. Los gráficos que siguen nos dan una idea clara del significado de cada una de estas funciones.



Ejemplo 1.8

Probar que $\lfloor -x \rfloor = -\lceil x \rceil$.

Solución: Supongamos que $\lfloor -x \rfloor = n$, es decir, $n \leq -x < n+1$. Entonces $-n-1 < x \leq -n$, es decir, $\lceil x \rceil = -n$. $\therefore$ $\lfloor -x \rfloor = -\lceil x \rceil$.

Ejemplo 1.9

Sea $n \in \mathbb{Z}$. Entonces $n = 2k$ o $n = 2k+1$ para algún entero k, ya sea que n es par o impar.

a.) Si $n = 2k+1 \geq 3$, entonces $\left[\!\left[\frac{n-3}{2}\right]\!\right] = \left[\!\left[\frac{2k-2}{2}\right]\!\right] = k-1$

b.) Si $n = 2k \geq 3$, entonces $\left[\!\left[\frac{n-3}{2}\right]\!\right] = \left[\!\left[\frac{2k-3}{2}\right]\!\right] = \left[\!\left[k-1-\frac{1}{2}\right]\!\right] = k-2$

c.) Si $p = 8k-1 > 3$, entonces $\frac{p-1}{2} - \left[\!\left[\frac{p}{4}\right]\!\right] = 4k-1-(2k-1) = 2k$

Ejemplo 1.10 (Conteo).

Si $x > 0$, el número $[\![x]\!]$ cuenta la cantidad de enteros positivos menores o iguales a x pues, por definición, si $[\![x]\!] = k$ entonces $1, 2, ..., k$ son menores que x.

Sea p un entero positivo y $x \geq p$. $[\![x/p]\!]$ cuenta la cantidad de enteros $\leq x$ divisibles por p. En efecto, los enteros positivos divisibles por p e inferiores a x son los k números $p < 2p < ... < k \cdot p \leq x$. Como $kp \leq x < (k+1)p$, entonces $k = [\![x/p]\!]$.

1.4 Números Poligonales y Piramidales

Los *números figurados* son enteros positivos que pueden ser representados por patrones geométricos. Los *números poligonales* son números figurados que se pueden representar por medio de polígonos regulares en el plano. Los *números piramidales* son números que pueden ser representados por formas piramidales. Ellos son obtenidos tomando sumas de los correspondientes números poligonales.

Números cuadrados. Los Pitagóricos usaban la palabra *gnomon* (=◢) para referirse a los enteros impares $1, 3, 5, 7, ...$. De manera figurada, cada gnomon es una "configuración" de puntos que se agrega a la configuración anterior, manteniendo su forma (figura 1.3). Ellos observaron que n^2 es la suma de los n primeros impares,

$$\begin{aligned} 1 &= 1^2, \\ 1+3 &= 2^2, \\ 1+3+5 &= 3^2, \\ 1+3+5+7 &= 4^2 \\ &\vdots \end{aligned}$$

En el ejemplo (1.2) ya habíamos indicado que Francesco Maurolico (1494-1575), probó este hecho usando por primera vez, inducción matemática. Una "prueba geométrica" se puede observar en la figura (1.3).

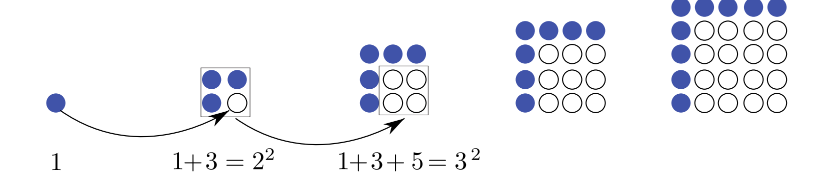


Figura 1.3. Cada cuadrado es construido agregando un número impar (los círculos azules)

Los *números cuadrados* s_n, corresponden a la cantidad de puntos en un arreglo cuadrangular de $n \times n$. En este caso $s_n = n^2$. A los números s_n también se les llama *cuadrados perfectos*, y como acabamos de ver, son una suma de números impares. También notamos en el ejemplo 1.2 que $s_{n+1} = s_n + 2n + 1$, es decir, el siguiente cuadrado perfecto se obtiene agregando *un gnomon* (la escuadra de $2n + 1$ puntos azules) al número figurado anterior.

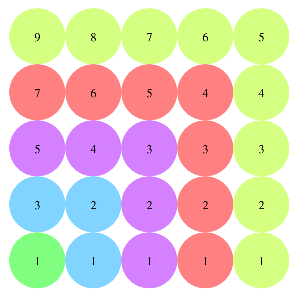
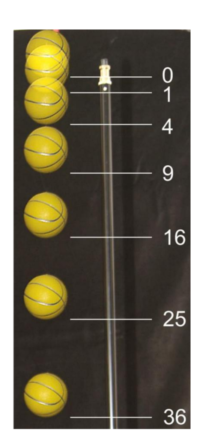


Figura 1.4. Cuadrados perfectos.

Ley de la caída de los cuerpos de Galileo. En 1590 Galileo estableció, usando relojes de agua, que un objeto inicialmente estacionario que se deja caer libremente por gravedad (ignorando resistencia del aire y rotación de la tieraa), cae una distancia que es proporcional al cuadrado del tiempo transcurrido. La imagen de la derecha, que abarca medio segundo, fue capturada con un flash estroboscópico en 20 destellos por segundo. Durante el primer 1/20 de segundo la bola cae una unidad de distancia (aquí, una unidad es aproximadamente 12 mm); a los 3/20 de segundo llevamos 4 unidades, a los 5/20 de segundo llevamos 9 unidades, a los 7/20 de segundo llevamos 16 unidades, etc. En general, un cuerpo cae en distancias proporcionales a los tiempos $1,\ 1+3,\ 1+3+5,1+3+5+7,...$ así que la distancia total de caída es proporcional al cuadrado del tiempo. La constante de proporcionalidad (cerca de la superficie de la tierra) es $0.5g$ y la la fórmula para la distancia recorrida en la caída es $d(t) = \frac{1}{2}gt^2$.



Números Triángulares. Los *números triangulares* t_n corresponden a la cantidad de círculos (o puntos u otra cosa) en un arreglo triangular con n columnas, como se ve en la figura (1.5).

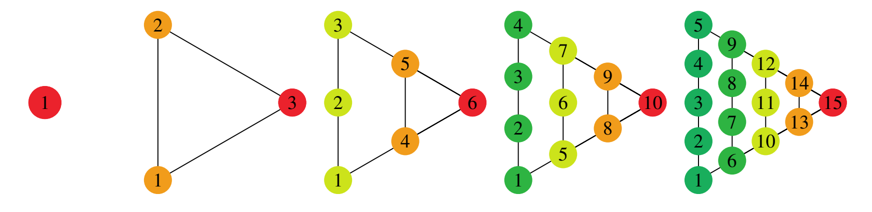


Figura 1.5. Números triangulares $t_1 = 1,\ t_2 = 3,\ t_3 = 6,\ t_4 = 10, ...$

Como cada columna tiene un elemento más que la columna anterior, tenemos que

$$t_n = 1 + 2 + \cdots + n - 1 + n$$

Podemos tomar dos copias de t_n y hacerlas encajar, de tal manera que obtengamos un rectángulo,como se ve en la figura (1.6).

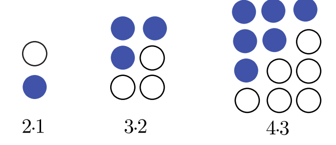


Figura 1.6. $2t_1 = 2 \cdot 1$, $2t_2 = 3 \cdot 2$, $2t_3 = 4 \cdot 3, \ldots$

Esto nos lleva de inmediato a la fórmula cerrada $t_n = \dfrac{n(n+1)}{2}$.

La figura (1.7) también constituye una "prueba geométrica" (base para una conjetura) de la relación entre números triangulares y cuadrados, $t_n + t_{n-1} = s_n$

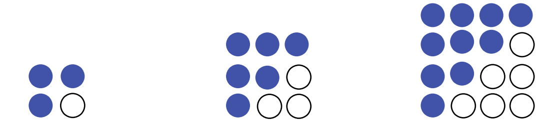
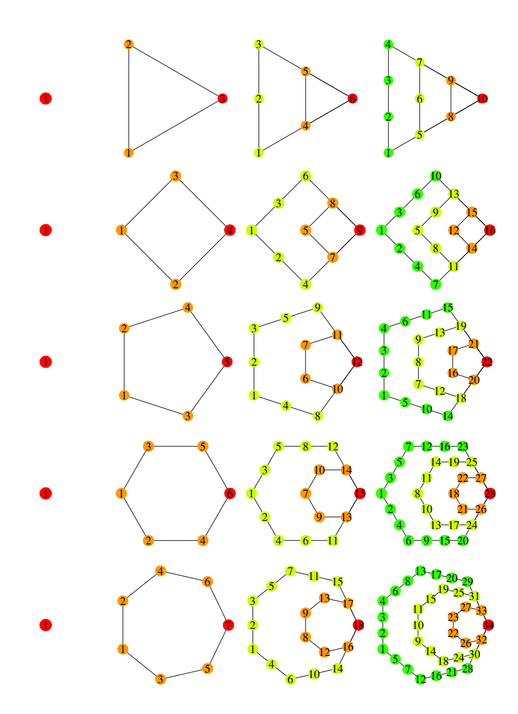


Figura 1.7. $t_n + t_{n-1} = s_n$

Es fácil responder la pregunta ¿Cuándo un número triangular es cuadrado?. Esto sucede si $t_n = s_m$, ahora usamos nuestras fórmulas,

$$t_n = s_m \iff \frac{n(n+1)}{2} = m^2 \iff (2n+1)^2 - 8m^2 = 1$$

En general, un número poligonal es un tipo de número figurado, que cuenta la cantidad de objetos en un arreglo en forma de cuadrado, triángulo, etc. La figura (1.8) muestra algunos de estos arreglos,



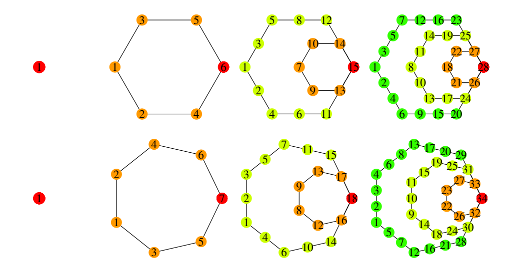


Figura 1.8. Números poligonales

Números tetraédricos. Denotados como T_n, son los análogos de los triangulares en 3D. Estos números son la cantidad de puntos en una pirámide tetraédica, como se observa en la figura (1.9),

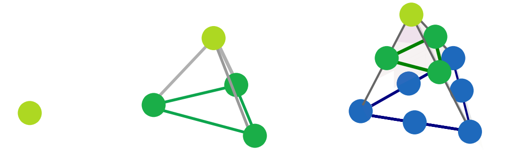


Figura 1.9. $T_1 = 1$, $T_2 = 4$, $T_3 = 10, \ldots$

Como la $n-$ésima capa es un arreglo triangular de t_n puntos, entonces

$$T_n = t_1 + t_2 + \ldots + t_n$$

La "prueba geométrica" es un poco más complicada. Se requiere usar cubos, en vez de puntos, de tal manera que varias copias encajen perfectamente para formar un cuboide. Por ejemplo, consideremos $T_3 = 10$, en la figura (1.10) se puede observar la nueva configuración de T_3 usando cubos. Las dos copias de T_3 ajustan bien, pero no constituyen un cuboide.

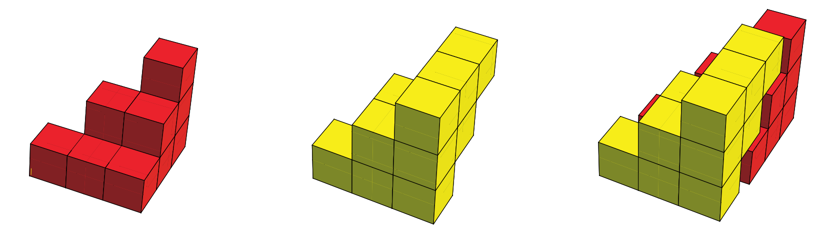


Figura 1.10. Encajar dos copias de $T_3 = 10$

Para lograr un cuboide necesitamos seis copias de T_3, como se ve en la en la figura (1.11)

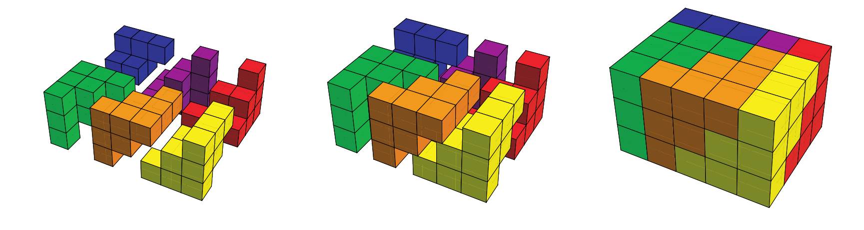


Figura 1.11. Encajando seis copias de $T_3 = 10$

Entonces, con seis copias de T_3 obtenemos un cuboide de orden $3\times(3+1)\times(3+2)$, por tanto $T_3 = 3(3+1)(3+2)/6$. Generalizando, si sumamos seis copias de T_n, obtenemos es un cuboide de orden $n\times(n+1)\times(n+2)$, es decir,

$$T_n = \frac{n(n+1)(n+2)}{6}$$

Números piramidales P_n de base cuadrada. Estos números corresponden a la cantidad de objetos en una pirámide de base cuadrada y altura n. En la figura (1.12) se muestra una configuración para $P_4 = 30$.

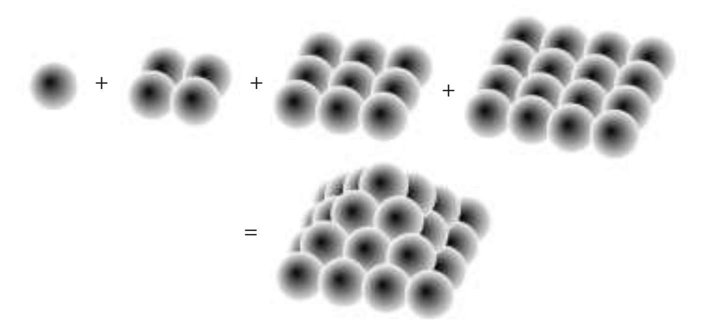


Figura 1.12. $P_4 = 30$

La $k-$ésima capa en la pirámide es un cuadrado con $s_k = k^2$ objetos, entonces

$$P_n = 1^2 + 2^2 + ... + n^2$$

Para obtener una fórmula para P_n, usamos la relación entre números cuadrados y números triangulares, esto nos lleva a una expresión en términos de T_n.

$$\begin{aligned} P_n &= \sum_{k=1}^{n} k^2 = \sum_{k=1}^{n}(t_k + t_{k-1}) \\ &= \sum_{k=1}^{n} t_k + \sum_{k=1}^{n} t_{k-1} = T_n + T_{n-1} \\ &= \frac{n(n+1)(2n+1)}{6}. \end{aligned}$$

EJERCICIOS

1.1 Verifique, usando el principio del buen orden, que el conjunto $S = \{2x+3y : x, y \in \mathbb{Z}\}$ tiene un elemento positivo mínimo y calcular este elemento.

1.2 Use un el área de un rectángulo $n\times(n+1)$ para modlar la suma $1+2+3+...+n = \dfrac{n(n+1)}{2}$

1.3 Sea $S = \{1,2,3,...,1000000\}$. ¿Cuántos números hay en S que son divisbles por 1021?.

1.4 Use el principio de Inclusión-Exclusión para establecer una fórmula, usando la función parte entera, que cuente todos los números positivos menores que x que *no* son divibles por 3 ni por 5. Luego use la fórmula para verificar que en el primer millón de naturales, hay 533333 números que *no* son divibles por 3 ni por 5. (Sugerencia: Contamos los números positivos divisibles únicamente por 3 y los divisibles únicamente por 5 y luego los excluimos. Usamos el principio de Inclusión-Exclusión para contar porque tenemos que excluir los que simúltaneamente son divisibles por 3 y 5.)

1.5 Probar, usando el principio de inducción, las fórmulas para s_n, t_n, y T_n

1.6 Muestre que $8t_n + 1 = s_{2n+1}$

1.7 Probar, usando inducción, que si a y n son enteros positivos, existe otro entero positivo m tal que $am > n$

1.8 Use inducción para probar que $1 + 2^3 + 3^3 + ... + n^3 = n^2(n+1)^2/4$

1.9 Probar la fórmula para la suma de los primeros n términos en una progresión aritmética,

$$a + (a+d) + (a+2d) + ... + [a + (n-l)d] = na + \frac{n(n-1)}{2}\,d$$

1.10 Probar que si $x \neq 1$ es un número real fijo, entonces

$$1 + x + x^2 + x^3 + \cdots + x^k = \frac{1 - x^{k+1}}{1-x},\ k \in \mathbb{N}$$

1.11 Mostrar que si $x \notin \mathbb{Z}$, entonces $\lceil\!\lceil x \rceil\!\rceil = \lfloor\!\lfloor x \rfloor\!\rfloor + 1$.

1.12 **[Truncamiento y redondeo.]** Sea $x \in \mathbb{R}$. La expansión decimal de x es,

$$x = a.a_1a_2a_3.... = a + a_1 \cdot 10^{-1} + a_2 \cdot 10^{-2} + a_3 \cdot 10^{-3} + ..., \quad \text{con} \quad a \in \mathbb{Z} \ \text{ y } \ a_i \in \{0,1,2,...,9\}.$$

Por ejemplo, $3.1415926535... = 3 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + 1 \cdot 10^{-3} + 5 \cdot 10^{-4} + \cdots$.

Probar que si $n \in \mathbb{N}^+$,

a) $\lfloor\!\lfloor 10^n\, x \rfloor\!\rfloor / 10^n$ es un truncamiento de x a n cifras decimales.
Por ejemplo, $\lfloor\!\lfloor 1000 \cdot 3.1415926535... \rfloor\!\rfloor / 1000 = 3.141$.

b) $\lfloor\!\lfloor 10^n\, x\ +\ 0.5 \rfloor\!\rfloor / 10^n$ es un redondeo de x a n cifras decimales.
Por ejemplo, $\lfloor\!\lfloor 1000 \cdot 3.1415926535...\ + 0.5 \rfloor\!\rfloor / 1000 = 3.142$.



2 DIVISIBILIDAD

Definición 2.1

Sean a, b enteros con $b \neq 0$. Decimos que b divide a a si existe un entero c tal que $a = bc$. Si b divide a a escribimos $b|a$

Teorema 2.1

Sean $a, b, d, p, q \in \mathbb{Z}$.

a.) Si $d|a$ y $d|b$ entonces $d|(ax+by)$ para cualquier $x, y \in \mathbb{Z}$

b.) Si $d|(p+q)$ y $d|p \implies d|q$.

c.) Si $a, b \in \mathbb{Z}^+$ y $b|a \implies a \geq b$

d.) Si $a|b$, entonces $a|mb$, con $m \in \mathbb{Z}$.

e.) Si $a, b \in \mathbb{Z}$, $a|b$ y $b|a \implies |a| = |b|$

Prueba:

a.) Sea $a = nd$ y $b = md$, entonces $ax + by = (nx + my)d \implies d|(ax+by)$

b.) Sea $p = kd$ y $p + q = k'd$, entonces $q = d(k' - k) \implies d|q$

c.) Como $a, b \in \mathbb{Z}^+$, si $a = kb$ entonces $k \geq 1$ y por tanto $a = bk \geq b$.

d.) Sea $b = ka \implies mb = mka = (mk)a \implies a|mb$

e.) El item **c.)** solo aplica si a y b son positivos. Si $a|b$ y $b|a$ entonces, $|a|\,||b|$ y $|b|\,||a|$, por el item **c.)**, $|a| \leq |b|$ y $|b| \leq |a|$. $\therefore$ $|a| = |b|$

Ejemplo 2.1

$5|-5$ y $-5|5.$ $\therefore$ $|5|=|-5|$

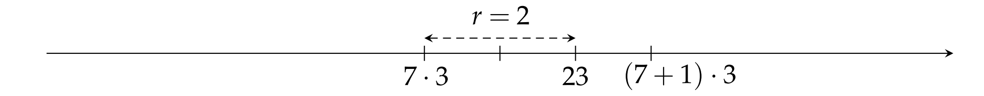
Ejemplo 2.2

Sean $a,b,d \in \mathbb{Z}$. Muestre que si $a|d$ y $d|b$ entonces $a|b$

Solución: Si $a|d \wedge d|b \implies d = k_1a \wedge b = k_2d,$ con $k_1,k_2 \in \mathbb{Z}$. Luego $b = k_2d = k_2(k_1a) \implies a|b$

2.1 "Algoritmo de la división"

Si la división no es exacta, no todo está perdido: Como hacíamos en la escuela, la división de a por b la podemos expresar como un cociente y un resto. Por ejemplo, la división de 23 por 3 es 7 y queda un resto $r=2$. Es decir, $23 = 7\cdot 3 + 2$. Gráficamente,



Teorema 2.2 (Teorema de la división).

Sean $a,b \in \mathbb{Z}$ con $b \neq 0$. Existen $q,r \in \mathbb{Z}$ únicos tales que

$$a = bq + r \quad \text{con} \quad 0 \leq r < |b|.$$

Prueba: Primero vamos a demostrar el teorema para $a,b \in \mathbb{Z}$ con $b > 0$. Consideremos la progresión aritmética

$$\ldots, -3b,\ -2b,\ -b,\ 0,\ b,\ 2b,\ 3b, \ldots$$

Por el principio del buen orden (ver el ejemplo 1.1) existe $q \in \mathbb{Z}$ tal que

$$qb \leq a < (q+1)b$$

r

qb $\quad a \quad$ $(q+1)b$

Sea $r = a - qb$, entonces $a = bq + r$. De $qb \leq a$ obtenemos $0 \leq r$ y de $a < (q+1)b \implies a - qb < b$. $\therefore a = bq + r$ con $0 \leq r < b$

Unicidad: La prueba es por contradicción. Supongamos que existe $q_1,\ r_1 \in \mathbb{Z}$ tal que

$$a = bq_1 + r_1 \quad \text{con} \quad 0 \leq r_1 < b \quad \text{y} \quad a = bq + r \quad \text{con} \quad 0 \leq r < b$$

Ahora supongamos que $r \neq r_1$ y que $r > r_1$.

$$\left\{\begin{array}{lcl} a & = & bq_1 + r_1 \\ a & = & bq + r \end{array}\right. \Longrightarrow bq_1 + r_1 \;-\; (bq + r) = 0 \Longrightarrow b(q_1 - q) = r - r_1 \Longrightarrow b|(r - r_1).$$

Como $b|(r - r_1)$, se tiene que $r - r_1 \geq b$; pero $0 < r - r_1 < r < b$; contradicción!.

Por lo tanto, $r = r_1$. De aquí: $b(q_1 - q) = r - r_1 = 0 \Longrightarrow q_1 = q$

Caso $b < 0$. Existen $q, r \in \mathbb{Z}$ únicos tales que $a = |b|q + r$ con $0 \leq r < |b|$ con lo que

$$a = b \cdot (-q) \;+\; r \;\text{ con }\; 0 \leq r < |b|.$$

Nota 1: Si $a, b \in \mathbb{Z}^+$, el 'algoritmo de la división' corresponde a la división usual. Si a o b es negativo, la división usual difiere del teorema de la división.

El enunciado del teorema de la división es adecuado para fines teóricos. Para efectos de cálculo es mejor enunciar el teorema de la división así:

Teorema 2.3

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Existe un único $r \in \mathbb{Z}$ tal que

$$\text{Si } b > 0,\; a = b\lfloor a/b \rfloor + r \;\text{ con }\; 0 \leq r < b.$$

$$\text{Si } b < 0,\; a = b\lceil a/b \rceil + r \;\text{ con }\; 0 \leq r < |b|.$$

En este contexto, a/b denota la división usual en $\mathbb{R}$.

Prueba: Si $b > 0$ entonces, por el teorema de la divisón, existe $q \in \mathbb{Z}$ tal que $qb \leq a < (q+1)b$, es decir $q = \lfloor a/b \rfloor$ y, por supuesto $r = a - b\lfloor a/b \rfloor$.

Si $b < 0$ entonces $a = b \cdot (-q) \;+\; r$ con $0 \leq r < |b|$. Así, $-q = -\lfloor a/b \rfloor = \lceil a/b \rceil$, por tanto $-q = \lceil a/b \rceil$ y, por supuesto $r = a - b\lceil a/b \rceil$.

Notación para restos. El *resto de la división* de a por b se denota "$\text{rem}\,(a, b)$" o también "$\text{rem}(a, b)$". Por supuesto, $a|b$ si $\text{rem}\,(a, b) = 0$. Para efectos teóricos puede ser conveniente que $r > 0$ pero en cálculos computacionales se puede permitir que r sea negativo. Esto es algo que vamos a retomar más adelante.

Ejemplo 2.3

Dividir -12 por -5:

$$\begin{array}{r|l} -12 & -5, \\ \hline 10 & 2 \\ \hline -2 & \end{array}$$

En la división ordinaria $-12 = 2 \cdot -5 - 2$.
Desde el punto de vista del teorema de la división, como $-3 \cdot 5 \leq -12 < -2 \cdot 5$, se tiene
$-12 = -3 \cdot 5 + 3$

Ejemplo 2.4

Si $a = 2q + r$ con $0 \leq r < 2$. Si $r = 0$ a se dice *par* y si $r = 1$, a se dice *impar*.

Ejemplo 2.5

Sean $n, p \in \mathbb{N}$ con $n \geq p > 0$. Mostrar que hay $\llbracket n/p \rrbracket$ números divisibles por p en el conjunto $A = \{1, 2, ..., n\}$.

Solución: Si $p < n$ entonces p divide a los números $\{p, 2p, ..., qp\} \subseteq A$ donde $qp \leq n < (q+1)p$, es decir p divide a $\llbracket n/p \rrbracket$ números en este conjunto.

Ejemplo 2.6

¿Cuántos enteros positivos ≤ 1000000 *no* son divisibles por 3 ni por 5?

Solución: Contamos los númerospositivos divisibles únicamente por 3 y los divisibles únicamente por 5 y luego los excluimos. Podemos usar el principio de Inclusión-Exclusión para contar porque tenemos que excluir los que simúltaneamente son divisibles por 3 y 5.

Sea $A = \{x \in \mathbb{Z}^+ : x \leq 1000000 \text{ y } 3|x\}$ y $B = \{x \in \mathbb{Z}^+ : x \leq 1000000 \text{ y } 5|x\}$. Los números divisibles por 3 y por 5 son divisibles por 15. Entonces,

$$\begin{aligned} |A \cup B| &= |A| + |B| - |A \cap B| \\ &= \llbracket 1000000/3 \rrbracket + \llbracket 1000000/5 \rrbracket - \llbracket 1000000/15 \rrbracket \\ &= 333333 + 200000 - 66666 = 466667 \end{aligned}$$

Por tanto, en el primer millón de enteros positivos, hay $1000000 - 466667 = 533333$ enteros *no* divisibles por 3 ni por 5.

EJERCICIOS

2.1 Dé un contraejemplo de la afirmación: $a|bc$ y $a \nmid c$ entonces $a|b$

2.2 Mostrar que si $d|a \wedge d|(a+1)$ entonces $|d|=1$

2.3 Sean $d,n \in \mathbb{Z}$. Si d no divide a n entonces ningún múltiplo de d divide a n.

2.4 Si $d|a$ y $d|b$ y si $a=bq+r$ entonces $d|r$.

2.5 Sea $b \neq 0$ y $a=qb+r$ con $0 \leq r < |b|$. Muestre que en el conjunto $\{a, a-1, ..., a-|b|+1\}$ hay un único múltiplo de b.

2.6 Muestre que si $a,b,d \in \mathbb{Z}$, a impar y si $d|a$ y $d|(ab+2)$, entonces $d=1$

2.7 ¿Cuántos enteros positivos ≤ 3000 son divisibles por 3, 5 o 7? **Ayuda:** $|A \cup B \cup C| = |A|+|B|+|C|-|A \cap B|-|B \cap C|-|C \cap A|+|A \cap B \cap C|$

2.2 Números Primos.

Definición 2.2 (Primos y compuestos).

Un entero $p>1$ se dice primo si sus únicos divisores son 1 y p. Si p no es primo, se dice compuesto.

El número 1 no se toma como primo solo por conveniencia. No perjudica en nada y obtenemos cierta economía en la formulación de teoremas.

Ejemplo 2.7

Los primeros primos son $\{2,3,5,7,11,13,17,...\}$

Ejemplo 2.8

Sea p_i el $i-$ésimo primo. El número $N = p_1 \cdot p_2 \cdot sp_n + 1$ puede ser o no ser primo. Por ejemplo,

$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \; + \; 1 = 2311$ es primo (ver ejemlo 2.9),

$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \; + \; 1 = 30031 = 59 \cdot 509$ no es primo.

Teorema 2.4

Todo entero positivo $n>1$ tiene un divisor primo

Prueba: Si n es primo, tiene un divisor primo (él mismo). Supongamos que n es compuesto. Por el principio del buen orden podemos suponer que existe un $d > 1$ que es el más pequeño divisor positivo de n. Entonces d es primo. En efecto, si d fuera compuesto, d tendría un divisor $1 < d_1 < d$. Pero si $d_1|d$ y $d|n$ entonces $d_1|n$, en contradicción con la suposición de que d era el más pequeño divisor > 1, de n.

Corolario 2.1 *Sea* $n \in \mathbb{Z}$, $n > 1$. *El más pequeño divisor positivo* $d > 1$ *de* n *es primo.*

¿Cómo decidir si n es primo? El problema de decidir si es un número es primo no es en general fácil. Si n es un número muy grande, probar que n no es divisible por ningún número excepto 1 y n, nos llevaría a hacer un número nada razonable de cálculos. El siguiente teorema nos dice que para determinar si un número n es primo o no, basta con probar con los divisores primos inferiores a $\sqrt{n}$. Aunque $\sqrt{n}$ es en general pequeño respecto a n, este método tiene un alcance muy limitado.

Teorema 2.5

Sean $a, b, n \in \mathbb{N}$, $a > 1$, $b > 1$ y $n > 1$.

a.) Si $n = ab$, entonces $a \leq \sqrt{n} \vee b \leq \sqrt{n}$.

b.) Si n *no* tiene divisores primos $\leq \sqrt{n}$, entonces n es primo.

Prueba: Probamos **a.)** por contradicción: Si $a > \sqrt{n} \wedge b > \sqrt{n} \Longrightarrow ab > n$. $(\Rightarrow\Leftarrow)$.

Probamos **b.)**: Si n fuera compuesto, $n = ab$ con $a > 1, b > 1$. Entonces como los divisores primos de a y b son divisores de n, tendríamos que al menos uno de eso divisores es menor que $\sqrt{n}$ en contradicción con la hipótesis.

Corolario 2.2 *Si* n *es compuesto,* n *tiene un divisor primo* $p \leq \sqrt{n}$.

Ejemplo 2.9

- ¿$n = 103$ es compuesto?

Solución: 103 es primo pues no es divisible por ningún primo inferior a $\sqrt{103} \approx 10.1$ En efecto, los primos inferiores a 10 son $2,3,5$ y 7. Para probar que n no es divisible por alguno de estos números calculamos los residuos: $\text{rem}(103,2) = 1$, $\text{rem}(103,3) = 1$, $\text{rem}(103,5) = 3$ y $\text{rem}(103,7) = 5$.

- ¿$n = 2311$ es primo?

Solución: Si es primo. En efecto, si no fuera primo, $n = 2311$ tendría un divisor primo p con $p \leq \sqrt{2311} = 48.07\ldots$. Los primos inferiores a 48 son $\{2,3,5,7,11,13,17,19,23,29,$

31, 37, 41, 43, 47} pero ninguno de ellos divide a 2311.

- ¿Puede un número n compuesto tener factores primos más grandes que $\sqrt{n}$?

Solución: Si $n = p_1 p_2$ con p_1 y p_2 primos distintos, no podrían ser ambos $< \sqrt{n}$!. Por ejemplo $206 = 2 \cdot 103$ y $103 > \sqrt{206} \approx 14.35$. Hay casos como $16 = 2 \cdot 2 \cdot 2 \cdot 2$ y $2 < \sqrt{16}$.

¿Cuántos primos hay?. Los primos son infinitos. Es algo que se conoce desde la época de Euclides.

Teorema 2.6 (Euclides).

Hay un número infinito de primos

Prueba: La demostración es por contradicción: Si $p_1, \ldots, p_n$ fueran todos los primos, el número $N = p_1 p_2 \cdot s p_n + 1$ es un nuevo primo o tiene un divisor primo diferente de cada p_i, $i = 1, 2, ..., n$. Si N es primo, $N > p_i$, $i = 1, 2, ..., n$ y entonces sería un nuevo primo, contradicción.. Si N no es un nuevo primo, tiene un divisor primo p_j, pero entonces como $p_j | (p_1 p_2 \cdot s p_n + 1)$ y $p_j | (p_1 p_2 \cdot s p_n) \implies p_j | 1$ lo cual es imposible pues $p_j > 1$.

¿Cuántos primos hay $\leq x$?. Ahora esta es la pregunta correcta. $\pi(x)$ denota la cantidad de primos inferiores o iguales x. Por ejemplo, $\pi(5) = \pi(6) = 3$. Hasta el 2008, se conocen todos los primos inferiores a $x = 100\,000\,000\,000\,000\,000\,000\,000 = 10^{23}$. Se tiene

$$\pi(10^{23}) = 1\,925\,320\,391\,606\,803\,968\,923.$$

También se conocen algunos primos fuera de éstos, por ejemplo $19249 \cdot 2^{13018586} + 1$ es un primo con 3918990 dígitos; fue encontrado en el 2007 por Samuel Yates.

Una fórmula (no muy eficiente) para $\pi(n)$ es la fórmula de Legendre (ver la sección 7.4.1),

Teorema 2.7 (Legendre).

Sean $p_1, p_2, ..., p_s$ los primos $\leq \sqrt{n}$, entonces

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_{1 \leq i \leq s} [\![n/p_i]\!] + \sum_{i<j} [\![n/(p_i p_j)]\!] - \sum_{i<j<k} [\![n/(p_i p_j p_k)]\!] + \cdots + (-1)^s [\![n/(p_1 p_2 \cdot s p_s)]\!].$$

Ejemplo 2.10

Calcular $\pi(100)$ con la fórmula de Legendre.

Solución: Los ingredientes son: $n = 100$, $\sqrt{100} = 10$, los primos ≤ 10 son $\{2,3,5,7\}$ y $\pi(\sqrt{100}) = 4$. Por tanto,

$$\begin{aligned}
\pi(100) &= 100 - 1 + 4 - (\lfloor\!\lfloor 100/2 \rfloor\!\rfloor + \lfloor\!\lfloor 100/3 \rfloor\!\rfloor + \lfloor\!\lfloor 100/5 \rfloor\!\rfloor + \lfloor\!\lfloor 100/7 \rfloor\!\rfloor) \\
&+ (\lfloor\!\lfloor 100/(2\cdot 3) \rfloor\!\rfloor + \lfloor\!\lfloor 100/(2\cdot 5) \rfloor\!\rfloor + \lfloor\!\lfloor 100/(2\cdot 7) \rfloor\!\rfloor + \lfloor\!\lfloor 100/(3\cdot 5) \rfloor\!\rfloor + \lfloor\!\lfloor 100/(3\cdot 7) \rfloor\!\rfloor \\
&+ \lfloor\!\lfloor 100/(5\cdot 7) \rfloor\!\rfloor) \\
&- (\lfloor\!\lfloor 100/(2\cdot 3\cdot 5) \rfloor\!\rfloor + \lfloor\!\lfloor 100/(2\cdot 3\cdot 7) \rfloor\!\rfloor + \lfloor\!\lfloor 100/(2\cdot 5\cdot 7) \rfloor\!\rfloor + \lfloor\!\lfloor 100/(3\cdot 5\cdot 7) \rfloor\!\rfloor) \\
&+ \lfloor\!\lfloor 100/(2\cdot 3\cdot 5\cdot 7) \rfloor\!\rfloor \;=\; 25.
\end{aligned}$$

2.3 Criba de Eratóstenes: Cómo colar números primos.

Como vimos en el ejemplo 2.9, se requiere conocer una lista de primos para decidir si un número es primo o no. Este método para determinar la primalidad de un número es conocido como 'ensayo y error' ('trial division'). Es efectivo para números pequeños pero no para números muy grandes. El problema es que la cantidad de números primos inferiores a $\sqrt{n}$ es aproximadamente $\sqrt{n}/\ln(\sqrt{n})$ (Teorema de los Números Primos), así por ejemplo si tenemos un número $a \approx 10^{20}$, para establecer si es primo o no, habría que probar con $\sqrt{10^{20}}/\ln(\sqrt{10^{20}}) \approx 4.34294 \times 10^8$ números primos..., es decir unos 434 millones de números. Aunque tuvieramos los números primos y un computador muy veloz, al sumar los tiempos que requiere cada división obtendríamos meses o años de cálculo. Más adelante veremos otras pruebas de primalidad.

Actualmente, la manera más eficiente de colar "*primos pequeños*", es usar la criba[1] de Eratóstenes. Este es un algoritmo que permite "colar" todos los números primos menores que un número natural dado n, eliminando los números compuestos de la lista $\{2, ..., n\}$. Es simple y razonablemente eficiente mientras no haya problemas de almacenamiento (este es su punto débil).

Primero tomamos una lista de números $\{2,3,...,n\}$ y eliminamos de la lista los múltiplos de 2. Luego tomamos el primer entero después de 2 que no fue borrado (el 3) y eliminamos de la lista sus múltiplos, y así sucesivamente. Los números que permanecen en la lista son los primos $\{2,3,5,7,...\}$.

[1] Criba, tamiz y zaranda son sinónimos. Una criba es un herramienta que consiste de un cedazo usada para limpiar el trigo u otras semillas, de impurezas. Esta acción de limpiar se le dice cribar o tamizar.

Ejemplo 2.11

Primos menores que $n=10$

Lista inicial	2	3	4	5	6	7	8	9	10
Eliminar múltiplos de 2	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
Resultado	2	3	5	7	9				
Eliminar múltiplos de 3	2	3	5	7	~~9~~				
Resultado	2	3	5	7					

Primer refinamiento: Tachar solo los impares. Excepto el 2, los pares no son primos, así que podríamos "tachar" solo sobre la lista de impares $\leq n$:

$$\{3,5,9,...,\} = \left\{2i+3 \;:\; i=0,1,... \left[\!\left[\frac{n-3}{2}\right]\!\right]\right\}$$

Para probar que esta lista efectivamente corresponde a los impares $\leq n$, observemos que el último impar es n o $n-1$. En cualquier caso, el último impar es $2\cdot\left[\!\left[\frac{n-3}{2}\right]\!\right]+3$ pues:

Si n es impar, $n=2k+1$ y $\left[\!\left[\frac{n-3}{2}\right]\!\right]=k-1 \implies 2(k-1)+3=n.$

Si n es par, $n=2k$ y $\left[\!\left[\frac{n-3}{2}\right]\!\right]=k-2 \implies 2(k-2)+3=2k-1=n-1.$

Segundo refinamiento: Tachar de p_k^2 en adelante. En el paso $k-$ésimo hay que tachar los múltiplos del primo p_k desde p_k^2 en adelante. Esto es así pues en los pasos anteriores se ya se tacharon $3\cdot p_k,\ 5\cdot p_k, ..., p_{k-1}\cdot p_k$. Por ejemplo, cuando nos toca tachar los múltiplos del primo 7, ya se han eliminado los múltiplos de 2,3 y 5, es decir, ya se han eliminado $2\cdot 7,\ 3\cdot 7,\ 4\cdot 7,\ 5\cdot 7$ y $6\cdot 7$. Por eso iniciamos en 7^2.

Tercer refinamiento: Tachar mientras $p_k^2 \leq n$. En el paso $k-$ésimo hay que tachar los múltiplos del primo p_k solo si $p_k^2 \leq n$. En otro caso, nos detenemos ahí. ¿Porque?. En el paso $k-$ésimo tachamos los múltiplos del primo p_k desde p_k^2 en adelante, así que si $p_k^2 > n$ ya no hay nada que tachar.

Ejemplo 2.12

Encontrar los primos menores que 20. El proceso termina cuando el cuadrado del mayor número confirmado como primo es <20.

a.) La lista inicial es $\{2,3,5,7,9,11,13,15,17,19\}$

b.) Como $3^2 \leq 20$, tachamos los múltiplos de 3 desde $3^2=9$ en adelante: $\{2,3,5,7,\not{9},11,13,\not{15},17,19\}$

c.) Como $5^2>20$ el proceso termina aquí: Primos <20: $\{2,3,5,7,11,13,17,19\}$

2.3.1 Algoritmo e implementación.

En este contexto, a/b denota división entera, es decir, a/b es el cociente de dividir a y b.

a.) Como ya vimos, para colar los primos en el conjunto $\{2,3,...,n\}$ solo consideramos los impares:

$$\{2i+3 \;:\; i=0,1,...[\![(n-3)/2]\!]\} = \{3,5,7,9,...\}$$

b.) Por cada primo $p=2i+3$ (tal que $p^2<n$), debemos eliminar los *múltiplos impares* de p menores que n, a saber

$$(2k+1)p=(2k+1)(2i+3), \quad k=i+1,i+2,...$$

Si $k=i+1$ entonces el primer múltiplo en ser eliminado es $p^2=(2i+3)(2i+3)$, como debe ser.

Esto nos dice que para implementar el algoritmo solo necesitamos un arreglo (booleano) de tamaño $[\![(n-3)/2]\!]$. En Java se pone "`(n-3)/2`" y en VBA se pone "`(n-3)\2`".

El arreglo lo llamamos `EsPrimo[i], i=0,1,...,(n-3)/2`.Cada entrada del arreglo "`EsPrimo[i]`" indica si el número $2i+3$ es primo o no.

Por ejemplo

`EsPrimo[0] = true` pues $n=2\cdot 0+3=3$ es primo,

`EsPrimo[1] = true` pues $n=2\cdot 1+3=5$ es primo,

`EsPrimo[2] = true` pues $n=2\cdot 2+3=7$ es primo,

`EsPrimo[3] = false` pues $n=2\cdot 3+3=9$ no es primo.

Si el número $p=2i+3$ es primo entonces $i=(p-3)/2$ y

`EsPrimo[(p-3)/2] = true.`

Si sabemos que $p=2i+3$ es primo, debemos poner

`EsPrimo[((2k+1)(2i+3) - 3)/2] = false`

pues estas entradas representan a los múltiplos $(2k+1)(2i+3)$ de p. Observe que cuando $i=0,1,2$ tachamos los múltiplos de 3,5 y 7; cuando $i=3$ entonces $2i+3=9$ pero en este momento `esPrimo[3]=false` así que proseguimos con $i=4$, es decir, proseguimos tachando los múltiplos de 11.

En resumen: Antes de empezar a tachar los múltiplos de $p = 2i + 3$ debemos preguntar si `esPrimo[i]=true`.

Algoritmo 2.1: Criba de Eratóstenes

```
Datos: n ∈ ℕ, n > 3
Salida: Primos entre 2 y n
máx= (n − 3)/2;
boolean esPrimo[i],  i = 1,2,...,máx;
for i = 1,2,...,máx do
    esPrimo[i] =True;
i = 0;
while (2i + 3)(2i + 3) ≤ n do
    k = i + 1;
    if esPrimo(i) then
        while (2k + 1)(2i + 3) ≤ n do
            esPrimo[((2k + 1)(2i + 3) − 3)/2] =False;
            k = k + 1;
    i = i + 1;
Imprimir;
Imprima 2, 3;
for j = 1,2,...,máx do
    if esPrimo[j] =True then
        Imprima 2j + 3
```

Nota: Es conveniente poner $(2i+3) \leq n/(2i+3)$ en vez de $(2i+3)(2i+3) \leq n$, para no operar con números innecesariamente grandes.

Hay variaciones de la criba de Eratóstenes muy eficientes ([15], [14],[20]). En la mayoría de las referencias elementales sobre esta criba no se eliminan los pares posiblemente por mantener la simplicidad y porque para estudios asintóticos no hay necesidad. La tabla que sigue muestra la diferencia en tiempos de ejecución (en segundos) en una implementación en MATHEMATICA[2]

Tiempo en segundos (en MATHEMATICA.).

n	Criba sin pares	Criba con pares
80000	1.10807	4.30427
90000	1.40809	5.49234
100000	1.67611	6.64842

Implementación en VBA Excel. El código que sigue hace la lectura de datos en un cuaderno como el que sigue. n se lee en la celda B7 y el número de columnas, para imprimir en formato de tabla, se lee en la columna C7. Se imprime desde la celda B9. La macro `Eratostenes(n, 9,`

[2]Esta implementación en MATHEMATICA se espera que sea lenta porque es un lenguaje interpretado.

2, CantidadColumnas) criba los primos e imprime. En este cuaderno la macro se ejecuta desde un botón (el cual se agrega desde la 'ficha del programador').

[Descargar]

	A	B	C	D	E	F	G
1							
2							
3							
4	Criba de Eratóstenes (ver código con Alt - F11)						
5							
6	Primos ≤	n	# columnas	Colar Primos			
7		100	6				
8							
9		2	3	5	7	11	13
10		17	19	23	29	31	37
11		41	43	47	53	59	61
12		67	71	73	79	83	89

```
Option Explicit
Public CantidadColumnasAnt As Integer
'Principal: Lectura de datos y llamada a la macro
Private Sub CommandButton1_Click()
   Dim n, CantidadColumnas

   n = Cells(7, 2)        'Lee n en celda B7
   CantidadColumnas = Cells(7, 3) 'Lee la cantidad de columnas en C7
   If n < 2 Then
      MsgBox ("El n\'umero digitado debe ser un n\'umero natural mayor que 3")
      Call LimpiaCeldas(9, 2, CantidadColumnas)
   ElseIf CantidadColumnas < 0 Or CantidadColumnas > 60000 Then
      MsgBox ("El n\'umero de columnas debe ser mayor a 0 y menor a 60 000")
      Call LimpiaCeldas(9, 2, CantidadColumnasAnt)
   Else
      Call Eratostenes(n, 9, 2, CantidadColumnas)
   End If
End Sub

Sub Eratostenes(n, fil, col, Optional CantidadColumnas As Variant)
   Dim i, j, k, pos, l
   Dim max As Integer

   Dim esPrimo() As Boolean
   If CantidadColumnas = "" Or CantidadColumnas = 0 Then
      CantidadColumnas = 10
   End If


   Call LimpiaCeldas(fil, col, CantidadColumnasAnt) 'Limpia celdas
   CantidadColumnasAnt = CantidadColumnas
   '**Criba---------------------------------------------------------*
```

```
   max = (n - 3) \ 2 'divisi\'on entera
   ReDim esPrimo(max + 1)


   For i = 0 To max
      esPrimo(i) = True
   Next i

   j = 0
   While (2 * j + 3) <= n\(2 * j + 3)
      k = j + 1
      If esPrimo(j) Then
         While (2 * k + 1) * (2 * j + 3) <= n
            pos = ((2 * k + 1) * (2 * j + 3) - 3) \ 2
            esPrimo(pos) = False
            k = k + 1
         Wend
      End If
      j = j + 1
   Wend
  '**-----------------------------------------------------------------*
  '**Imprimir en la hoja Excel-------------------------------------*
   Cells(fil, col) = 2
   'Hay dos casos especiales
   If CantidadColumnas = 1 Then
      Cells(fil + 1, col) = 3 : k=2 : j=0
   ElseIf CantidadColumnas = 2 Then
      Cells(fil, col + 1) = 3 : k=1 : j=0
   Else
      Cells(fil, col + 1) = 3 : k=0 : j=2
   End If
   For i = 1 To max
      If esPrimo(i) Then
         Cells(fil + k, col + j) = 2 * i + 3
         If CantidadColumnas <> 1 Then
            k = k + j \ (CantidadColumnas - 1)
            j = j + 1
            j = j Mod CantidadColumnas
         Else
            k = k + 1
         End If
      End If
   Next i
End Sub

Private Sub LimpiaCeldas(fil, col, nc)
   Dim k, j
   k = 0
   While LenB(Cells(fil + k, col)) <> 0
```

```
    For j = 0 To nc
       Cells(fil + k, col + j) = ""
    Next j
    k = k + 1
  Wend
End Sub
```

2.4 Máximo común divisor

Si a,b son enteros no ambos nulos, entonces d es un divisor común de a y b si $d|a$ y $d|b$. Denotamos con D_a al conjunto de divisores de a y con D_b el conjunto de divisores de b. Estos conjuntos no son vacíos pues al menos $1 \in D_a$ y $1 \in D_b$. El máximo común divisor común de a y b es el más grande entero positivo del conjunto $D_a \cap D_b$.

Ejemplo 2.13

Como $D_{-3} = \{-3,-1,1,3\}$ y $D_6 = \{\pm 6, \pm 3, \pm 2, \pm 1\}$, entonces $D_a \cap D_b = \{-3,3,-1,1\}$. Por tanto, el máximo común divisor de 3 y 6 es 3.

Antes de continuar, una pregunta: ¿porqué a y b no pueden ser ambos nulos?

Una definición más técnica y apropiada para el desarrollo teórica es,

Definición 2.3 (Máximo Común Divisor).

Sean a, b enteros con al menos uno de los dos diferente de cero. El máximo común divisor de a y b, denotado $\text{mcd}\,(a,b)$, es el entero *positivo* d que satisface:

a.) $d|a$ y $d|b$

b.) Si $c|a$ y $c|b$, entonces $c|d$

Si $\text{mcd}(a,b) = 1$ se dice que a y b son relativamente primos o simplemente "coprimos".

Ejemplo 2.14

$\text{mcd}\,(3,6) = \text{mcd}\,(-3,6) = \text{mcd}\,(3,-6) = 3.$

Ahora establecemos algunas propiedades útiles. Otras propiedades serán enunciadas más adelante, cuando tengamos más herramientas para hacer las pruebas.

Teorema 2.8

Sean $a,b \in \mathbb{Z}$, no ambos nulos.

a.) $\text{mcd}\,(a,0) = |a|$ si $a \neq 0$

b.) $\text{mcd}\,(a,b) = \text{mcd}\,(|a|,|b|)$

c.) Si $d = \text{mcd}\,(a,b)$, entonces $\text{mcd}\,(a/d,\, b/d) = 1$

d.) Si $d = \text{mcd}\,(a,b)$, entonces $\text{mcd}\,(a,b-na) = d$ con $n \in \mathbb{Z}$

Prueba: : Para probar **a.)** sea $d = \text{mcd}\,(a,0)$. Como $|a|\,|a$ y $|a|\,|0$, entonces $|a|\,|d$. Pero $d|\,|a| \implies d \leq |a|$. $\therefore$ $d = |a|$.

Para probar **b.)** sea $d = \text{mcd}(a,b)$ y $d_1 = \text{mcd}(|a|,|b|)$. Como $d|a \wedge d|b \implies d|\,|a| \wedge d|\,|b| \implies d|d_1$. Ahora como $d_1|\,|a| \wedge d_1|\,|b| \implies d_1|a \wedge d_1|b \implies d_1|d$. $\therefore$ $d = d_1$ por ser ambos positivos.

Para probar **c.)**, sea $d' = \text{mcd}\,(a/d,\, b/d)$, entonces hay enteros k,k' tales que $a/d = kd'$ y $b/d = k'd'$. Por tanto, $a = dkd'$ y $b = dk'd'$, es decir, $dd'|a \wedge dd'|b \implies dd' \leq d$ por definición; entonces d' es un entero positivo ≤ 1, es decir, $d' = 1$.

Para probar **d.)**, sea $d_1 = \text{mcd}(a,b-na)$. Como $d|a \wedge d|b \implies d|(b-na)$ por el teorema 2.1 **a.)**. Entonces $d \leq d_1$. Como $d_1|a \implies d_1|na$. Así $d_1|na \wedge d_1|(b-na) \implies d_1|b$ por el teorema 2.1 **b.)**. Entonces $d_1 \leq d$. $\therefore$ $d = d_1$

Nota. El orden importa. En el ejercicio 2.9 se pide dar un par de ejemplos que muestren que en general, si $d = \text{mcd}\,(a,b)$, entonces $d \neq \text{mcd}\,(a,a-nb)$ con $n \in \mathbb{Z}$

Ejemplo 2.15

Muestre que si p es primo, $\text{mcd}\,(a,p) = p$ o $\text{mcd}\,(a,p) = 1$.

Solución: Si $d = \text{mcd}\,(a,p)$, en particular $d|p$, por tanto, como p es primo, $d = 1 \vee d = p$.

Ejemplo 2.16

Muestre que si $n > 1$, p es primo y $p|(n^2+1)$, entonces $\text{mcd}\,(p,n) = 1$.

Solución: $\text{mcd}\,(p,n) = 1 \vee \text{mcd}\,(p,n) = p$. Si $\text{mcd}\,(p,n) = p$ entonces $p|n \implies p|n^2$ y como $p|(n^2+1)$ entonces $p|1$; contradicción. $\therefore$ $\text{mcd}\,(p,n) = 1$.

Ejemplo 2.17

Sea $d = \text{mcd}(a,b)$. Si $a = kd$ y $b = k'd$, entonces $\text{mcd}(k,k') = 1$.

Solución: El teorema 2.8 **c.)** dice que $\text{mcd}(a/d,\ b/d) = 1$, es decir, $\text{mcd}(k,k') = 1$.

En la práctica necesitamos calcular el máximo común divisor de varios números. Esto no es problema, el siguiente teorema nos dice que el máximo común divisor de varios números se puede calcular de la misma manera en la que sumamos: De dos en dos.

Teorema 2.9

Sean $a_1, a_2, .., a_n \in \mathbb{Z}^+$, $n \geq 3$. Entonces $\text{mcd}(a_1, a_2, ..., a_n) = \text{mcd}(a_1, \text{mcd}(a_2, ..., a_n))$.

Prueba: Sea $d = \text{mcd}(a_1, a_2, ..., a_n)$ y $d_1 = \text{mcd}(a_1, d_2)$ con $d_2 = \text{mcd}(a_2, ..., a_n)$. Como $d|a_1$, $d|a_2, ..., d|a_n$, entonces $d|d_2$ y por tanto $d|d_1$. Como $d_1|a_1$ y $d_1|d_2$ entonces $d_1|a_1$, $\wedge\ d_1|a_2, ..., d_1|a_n$ (por transitividad). Por tanto $d_1|d$ $\therefore$ $d = d_1$.

Corolario 2.3 *Sean $a_1, ..., a_n \in \mathbb{Z}$ no todos nulos, si*

$$\left.\begin{array}{rcl} \text{mcd}(a_1,a_2) & = & d_2, \\ \text{mcd}(d_2,a_3) & = & d_3, \\ & \cdots & \\ \text{mcd}(d_{n-1},a_n) & = & d_n, \end{array}\right\} \Longrightarrow d_n = \text{mcd}(a_1, ..., a_n).$$

Ejemplo 2.18

$\text{mcd}(3,6,12) = \text{mcd}(\text{mcd}(3,6),12) = \text{mcd}(3,12) = 3.$

2.5 Algoritmo de Euclides I.

El algoritmo de Euclides se basa en la aplicación sucesiva del siguiente lema

Lema 2.1

Sean $a,b,q,r \in \mathbb{Z}$ tales que $a = bq + r$ con $b > 0$ y $0 \leq r < b$. Entonces $\text{mcd}(a,b) = \text{mcd}(b,r)$.

Prueba: Según el teorema 2.8 **d.)**, $\text{mcd}(b,a) = \text{mcd}(b, a - bq) = \text{mcd}(b,r)$

Este resultado lo podemos usar para obtener un algoritmo para calcular el máximo común divisor de dos números.

Algoritmo de Euclides. Sean a y b números naturales, $b \neq 0$. Aplicando el teorema de la división se obtiene una sucesión finita $a,\ r_0 = b, r_1, r_2, ..., r_n,\ 0$ definida por

$$
\begin{aligned}
a &= r_0 q_1 + r_1, & 0 \leq r_1 < r_0 \\
r_0 &= r_1 q_2 + r_2, & 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, & 0 \leq r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, & 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0 & r_{n+1} = 0.
\end{aligned}
$$

El último término es $r_n = \text{mcd}(a, b)$.

Correctitud del algoritmo. Aplicando el teorema de la división obtenemos una sucesión decreciente de residuos $0 \leq ... < r_k < r_{k-1} < ... < r_1 < r_0 = b$. La sucesión es finita pues entre 0 y $r_0 \neq 0$ solo puede haber un número finito de enteros. Por tanto algún residuo debe ser cero (sino, se podría aplicar el teorema de la división indefinidamente y tendríamos una sucesión infinita de enteros entre 0 y b, lo cual es imposible.) Si $b|a$, entonces $r_1 = 0$ y r_0 sería el mínimo residuo positivo. En general, debe haber un residuo mínimo $r_n > 0$ y $r_{n+1} = 0$

De acuerdo al lema (2.1) tenemos que

$$
\begin{aligned}
\text{mcd}(a, b) &= \text{mcd}(a - r_0 q, r_0) \\
&= \text{mcd}(r_1, r_0) \\
&= \text{mcd}(r_1, r_0 - r_1 q_2) \\
&= \text{mcd}(r_1, r_2) \\
&= \text{mcd}(r_1 - r_2 q_2, r_2) \\
&= \text{mcd}(r_3, r_2) \\
&\vdots \\
&= \text{mcd}(r_{n-1}, r_n) \\
&= \text{mcd}(r_n, 0) = r_n
\end{aligned}
$$

Ejemplo 2.19

Vamos a aplicar el algoritmo de Euclides para calcular $\text{mcd}(8, 2)$ y $\text{mcd}(78, 32)$.

a.) $\text{mcd}\,(8,2) = 2$. En efecto;

$$8 = 2 \cdot 4 + 0$$

Así, $r_0 = 2$ y $r_1 = 0$.

b.) $\text{mcd}\,(78,32) = 2$. En efecto;

$$\begin{aligned} 78 &= 32 \cdot 2 + 14 \\ 32 &= 14 \cdot 2 + 4 \\ 14 &= 4 \cdot 3 + \textcircled{2} \\ 4 &= 2 \cdot 2 + 0 \end{aligned}$$

2.5.1 Algoritmo e implementación.

Recordemos que $\text{mod}(a,b)$ denota el resto de la división de a por b. En este algoritmo, en cada paso $r = \ \text{mod}\,(r_{n+1}, r_n)$ donde $r_{n+1} = c$ es el dividendo actual y $r_n = d$ es el divisor actual. Luego se actualiza $r_{n+1} = d$ y $d = r$. El proceso continúa mientras d no se anule.

Algoritmo 2.2: Máximo común divisor

Datos: $a, b \in \mathbb{Z}.\ b \neq 0$
Salida: $\text{mcd}\,(a,b)$

$c = |a|,\ d = |b|$;
while $d \neq 0$ **do**
  $r = \text{mod}(c,d)$;
  $c = d$;
  $d = r$;
return $\text{mcd}\,(a,b) = |c|$;

Implementación en VBA Excel.

```
Function mcd(a, b)
   Dim c As Long, d As Long, r As Long 'max = 2 147 483 647
      c = Abs(a)
      d = Abs(b)
   While d <> 0
      r = c Mod d 'residuo entre (c,d)
      c = d
      d = r
   Wend
   mcd = Abs(c)
End Function
```

Para calcular el mcd de una lista de enteros que están en una *columna* de una hoja de Excel, se puede seleccionar la lista con el ratón y convertir la lista a un vector de enteros. Luego aplicamos el algoritmo.

```
Private Sub mcdLista()
   Dim n, i
```

```
   Dim Rango As Range
   Dim Lista() As Long
   'Seleccionar rango y convertir a Array
   Set Rango = Selection
   n = Rango.Rows.Count 'Solo filas
   If n <= 1 Then
      MsgBox ("Debe seleccionar 2 o m\'as enteros")
      Exit Sub
   End If
   ReDim Lista(n)
   For i = 1 To n 'Arreglos inician en cero, rangos en 1
      Lista(i) = Rango(i, 1)
   Next i
   Cells(7, 6) = mcd_Lista(Lista)
End Sub
'Los arreglos se pasan solo por referencia
Function mcd_Lista(ByRef L() As Long) 'ByRef = por referencia
   Dim c As Long
   Dim i, n
   c = 0
   n = UBound(L) 'tamano del arreglo


   For i = 1 To n
      If c = 0 Then
         c = mcd(c, L(i))
      Else
         c = Abs(c) * Abs(L(i)) / mcd(c, L(i))
      End If
   Next i
   mcd_Lista = Abs(c)
End Function
```

2.6 Algoritmo Extendido de Euclides.

El siguiente teorema establece la llamada "Identidad de Etienne Bezout" aunque el resultado lo descubrió primero el francés Claude Gaspard Bachet de Méziriac (1581-1638).

Teorema 2.10 (Identidad de Bézout).

Si a,b son dos enteros no ambos cero, existen $s,t \in \mathbb{Z}$ (posiblemente no únicos) tales que

$$sa + tb = \operatorname{mcd}(a,b)$$

Prueba: Sea A el conjunto de combinaciones lineales enteras de a y b, $A = \{ua + vb : u,v \in \mathbb{Z}\}$. Este conjunto tiene números positivos, negativos y el cero. Sea $m = ax + by$ el más pequeño

entero positivo en A.

¿m divide a a y a b?. Mmmmm, supongamos que $a = mq + r$ con $0 \leq r < m$. Entonces,

$$0 \leq r = a - mq = a - (ax + by)q = (1 - qx)a + (-qy)b$$

Así, r es una combinación lineal de a y b, es decir, $r \in A$. Pero $0 \leq r < m$, así que la única posibilidad es que $r = 0$ por ser m el mínimo entero positivo en A.

Luego, $a = mq$ y $m|a$. De manera análoga podemos establecer que $m|b$. Sea $d = \operatorname{mcd}(a,b)$. Como m es común divisor de a y b, entonces $d \geq m$. Pero, como $a = k_1 d$ y $b = k_2 d$ entonces $m = ax + by = (xk_1 + yk_2)d > 0$, por lo tanto $m \geq d$. Así que $m = d$.

Los siguientes corolarios son sumamente útiles,

Corolario 2.4 *El* $\operatorname{mcd}(a,b)$ *es el más pequeño entero positivo de la forma* $sa + tb$; $s,t \in \mathbb{Z}$. *En particular,* $\operatorname{mcd}(a,b) = 1$ *si y sólo si existen* $x,y \in \mathbb{Z}$ *tal que* $ax + by = 1$

Prueba: Ejercicio.

Corolario 2.5 *Si* $a|bc$ *y* $\operatorname{mcd}(a,b) = 1$ *entonces* $a|c$.

Prueba: Como $\operatorname{mcd}(a,b) = 1$, existen $x,y \in \mathbb{Z}$ tal que $xa + by = 1$. Multiplicando por c a ambos lados,

$$acx + bcy = c$$

Como $a|ac$ y $a|bc$ entonces $a|(acx + bcy)$. $\quad \therefore a|c$.

Ejemplo 2.20

Si n es entero positivo, verifique que $\dfrac{n+2}{n+1}$ es irreducible.

Solución: Si $n > 0$, $n + 2 - (n+1) = 1$; entonces, según el corolario (2.4), $\operatorname{mcd}(n+2, n+1) = 1$.

Calcular t y s. La ecuación $sa + tb = \operatorname{mcd}(a,b)$ no tiene solución única para s,t enteros. Se puede obtener una solución despejando los residuos, en el algoritmo de Euclides, y haciendo una sustitución hacia atrás.

Consideremos la sucesión $r_1, r_2, ..., r_n$ del algoritmo de Euclides. Todos estos residuos son una combinación lineal entera de a y b: En efecto, como $r_1 = a - bq_0$ y $b = r_1 q_1 + r_2$ entonces r_2 es combinación lineal de a y b. Como r_1 y r_2 son combinaciones lineales de a y b y como $r_1 = r_2 q_2 + r_3$ entonces r_3 es combinación lineal de a y b. Continuando de esta manera, como r_{i-1} y r_{i-2} son combinaciones lineales de a y b y como $r_{i-2} = r_{i-1} q_2 + r_i$ $(i = 2, ..., n)$, entonces r_n es combinación lineal (mínima) de a y b.

Ejemplo 2.21

$\text{mcd}(78,32) = 2$. De acuerdo a la identidad d Bézout, existen $s,t \in \mathbb{Z}$ tal que $s \cdot 78 + t \cdot 32 = 2$. En este caso, una posibilidad es $7 \cdot 78 - 17 \cdot 32 = 2$, es decir $s = 7$ y $t = -17$.

s y t se pueden obtener así: Primero despejamos los residuos en el algoritmo de Euclides de abajo hacia arriba, iniciando con el máximo común divisor. Luego hacemos sustitución hacia atrás, sustituyendo las expresiones de los residuos. En cada paso se ha subrayado el residuo que se sustituye

$$\begin{array}{rcl} 78 &=& 32\cdot 2+14 \\ 32 &=& 14\cdot 2+4 \\ 14 &=& 4\cdot 3+2 \\ 4 &=& 2\cdot 2+0 \end{array} \begin{array}{c} \longrightarrow \\ \longrightarrow \\ \longrightarrow \\ \end{array} \begin{array}{rcl} 14 &=& 78-32\cdot 2 \\ 4 &=& 32-14\cdot 2 \;\uparrow \\ 2 &=& 14-4\cdot 3 \;\uparrow \\ && \end{array} \Longrightarrow \begin{array}{rcl} 2 &=& 14-\underline{4}\cdot 3 \\ &=& 14-(32-14\cdot 2)3 \\ &=& \underline{14}\cdot 7-32\cdot 3 \\ &=& (78-32\cdot 2)7-32\cdot 3 \\ &=& \underbrace{7}_{s}\cdot 78+\underbrace{-17}_{t}\cdot 32 \end{array}$$

Ejemplo 2.22

Calcular $s,t \in \mathbb{Z}$ tal que $s \cdot -8 + t \cdot 22 = \text{mcd}(-8,22)$.

Solución:

Calcular $\text{mcd}(-8,22)$

$$\begin{array}{rcl} -8 &=& -1\cdot 22+14 \\ 22 &=& 1\cdot 14+8 \\ 14 &=& 1\cdot 8+6 \\ 8 &=& 1\cdot 6+2 \\ 6 &=& 3\cdot 2+0 \end{array}$$

Cálculo de s y t

$$\begin{array}{rcl} 2 &=& 8-6 \\ &=& 8-(14-8) \\ &=& 8\cdot 2-\underline{14} \\ &=& 8\cdot 2-\underline{(-8+22)} \\ &=& 8\cdot 3-22 \\ &=& -8\cdot -3+-1\cdot 22 \\ \therefore && s=-3 \text{ y } t=-1 \end{array}$$

2.6.1 Algoritmo e implementación.

En este contexto, a/b denota el cociente de dividir a por b. El agoritmo implementa la sustitución hacia atrás que vimos antes.

Algoritmo 2.3: Algoritmo Extendido de Euclides

Datos: a, b enteros no ambos nulos

Salida: mcd (a,b), t y s

$c = |a|$, $d = |b|$;

$c_1 = 1$, $d_1 = 0$;

$c_2 = 0$, $d_2 = 1$;

while $d \neq 0$ **do**

$\quad q = c/d, \quad r = c - qd,$

$\quad r_1 = c_1 - qd_1, \quad r_2 = c_2 - qd_2,$

$\quad c = d, \quad c_1 = d_1, \quad c_2 = d_2,$

$\quad d = r, \quad d_1 = r_1, \quad d_2 = r_2,$

return mcd (a,b) $= |c|$, $\ s = c_1/\text{sgn}(a) \cdot \text{sgn}(c)$, $\ t = c_2/\text{sgn}(b) \cdot \text{sgn}(c)$;

Recordemos que $\text{sgn}(x) = \begin{cases} 1 & \text{si} \quad x \geq 0 \\ -1 & \text{si} \quad x < 0 \end{cases}$.

Validez del algoritmo. La validez de este algoritmo se establece probando que en todo el ciclo `While`, se tiene

$$\begin{aligned} c &= c_1\,|a| + c_2\,|b| \\ d &= d_1\,|a| + d_2\,|b| \end{aligned} \tag{2.1}$$

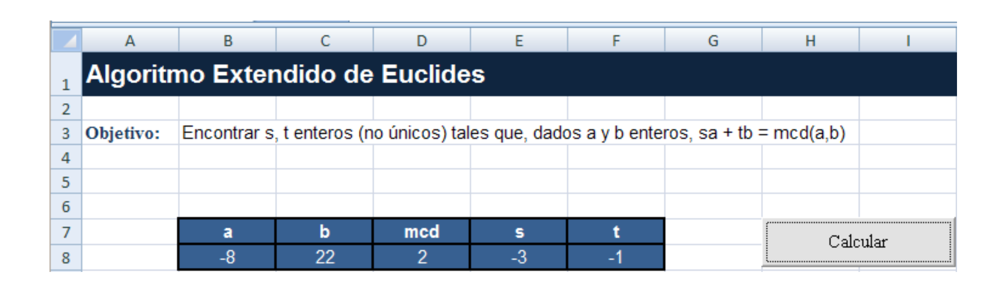
Al final, cuando $d = 0$, obtenemos s y t usando los datos en (2.1).

Como $|x| = x/\text{sgn}(x) = x \cdot \text{sgn}(x)$, entonces

$$\begin{aligned} |c| &= \frac{c_1}{\text{sgn}(c)}\,|a| + \frac{c_2}{\text{sgn}(c)}\,|b| \\ &= \underbrace{\frac{c_1}{\text{sgn}(c) \cdot \text{sgn}(a)}}_{s}\,a + \underbrace{\frac{c_2}{\text{sgn}(c) \cdot \text{sgn}(b)}}_{t}\,b \end{aligned}$$

Implementación en VBA Excel. Primero debemos implementar una función signo acorde con nuestra definición. Luego implementamos el algoritmo tal cuál.

[Descargar]




```
Option Explicit
Private Sub Calcular_Click()
   Dim a, b
   Dim vector() As Long
   a = Cells(8, 2) : b = Cells(8, 3)
   vector = EuclidesExtendido(a, b)
   Cells(8, 4) = vector(1) : Cells(8, 5) = vector(2) : Cells(8, 6) = vector(3)
End Sub
Function signo(x)
   If x < 0 Then
       signo = -1
   Else signo = 1
   End If
End Function
   Dim mcdst() As Long
   Dim c, c1, c2, d, d1, d2, q, r, r1, r2
   ReDim mcdst(3)

Function EuclidesExtendido(a, b) As Long()

   c = Abs(a) : d = Abs(b)
   c1 = 1 : c2 = 0
   d1 = 0 : d2 = 1
   While d <> 0
      q = c \ d
      r = c - q*d
      r1 = c1 - q*d1
      r2 = c2 - q*d2
      c = d : c1 = d1 : c2 = d2
      d = r : d1 = r1 : d2 = r2
   Wend
   mcdst(1) = Abs(c)              'mcd(a,b)
   mcdst(2) = c1 * signo(a) * signo(c) 's
   mcdst(3) = c2                  't
   EuclidesExtendido= mcdst()
End Function
```

2.7 Ecuaciones Diofánticas lineales.

Consideremos el problema de resolver $ax+by=c$ en enteros. Aquí a,b,c son dados y se debe determinar $x,y\in\mathbb{Z}$. Las condiciones de existencia de soluciones y el método para obtenerlas se basa en el algoritmo extendido de Euclides.

Ejemplo 2.23

Consideremos la ecuaciones en enteros $2x+3y=2$ y $6x-3y=1$ Gráficamente, las soluciones enteras corresponden a los pares $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ contenidos en la representación gráfica de cada recta.

En el caso de $2x+3y=2$, en la figura (2.1), se puede observar que $(-5,4)$, $(-2,2)$, $(1,0)$, $(4,-2)$, $(7,-4)$ son algunas soluciones. En el caso de la recta $6x-3y=1$, no se observan soluciones; ¿tendrá alguna?

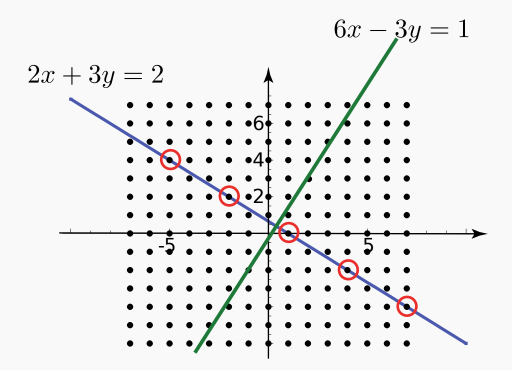


Figura 2.1. Algunas soluciones enteras de la ecuación $2x+3y=2$.

Teorema 2.11

La ecuación diofántica lineal $ax+by=c$ tiene soluciones $x,y\in Z$ si y sólo si $\operatorname{mcd}(a,b)|c$

Prueba: Sea $d=\operatorname{mcd}(a,b)$
"$\Longrightarrow$": Si existen $x,y\in\mathbb{Z}$ tal que $c=ax+ay$, entonces $d|c$ pues $d|a$ y $d|b$.
"$\Longleftarrow$": Si $d|c$ entones $c=kd$. Como podemos determinar, usando el algoritmo extendido de Euclides, $s,t\in\mathbb{Z}$ tal que $d=sa+tb$, entonces $c=kd=(ks)a+(kt)b$ y una solución de la ecuación diofántica lineal sería $x=ks$ y $y=kt$.

Ejemplo 2.24

La ecuación en enteros $2x+3y=2$ tiene solución pues $\operatorname{mcd}(2,3)=1$ y $1|2$. La ecuación en enteros $6x-3y=1$ no tiene soluciones enteras pues $\operatorname{mcd}(6,3)=3$ y $3\nmid 1$.

Ejemplo 2.25

Calcule una solución para la ecuación en enteros $-8x+22y=20$

Solución: En el ejemplo (2.21) encontramos que $2=\text{mcd}(-8,22)$ y que $2=-3\cdot -8+-1\cdot 22$. Ahora, como $20=2\cdot 10$,

$$2=-3\cdot -8\ +-1\cdot 22 \implies 20=-30\cdot -8+-10\cdot 22.$$

Así, una solución de la ecuación diofántica es $x=-30 \wedge y=-10$.

Solución general. La solución general se establece al estilo de las ecuaciones diferenciales y el álgebra lineal: Primero se busca la solución de la ecuación homogénea $ax+by=0$ y la solución general de la ecuación $ax+by=c$ se expresa usando esta solución.

Teorema 2.12

Sea $d=\text{mcd}(a,b)$. Las soluiones de la ecuación diofántica lineal homogénea $ax+by=0$ son de la forma,

$$x=\frac{b}{d}\,t, \qquad y=-\frac{a}{d}\,t \;\text{ con }\; t\in\mathbb{Z}.$$

Prueba: Claramente $\frac{a}{d}$ y $\frac{b}{d}$ son enteros. Sustituyendo directamente x e y se observa que efectivamente son soluciones de la ecuación homógenea para cualquier $t\in\mathbb{Z}$.

Ahora hay que mostrar que cualquier otra solución $x,y\in\mathbb{Z}$ tiene esa forma. Sea $a=kd$ y $b=k'd$. $ax+by=0 \implies ax=-by \implies kx=-k'y$. Esto último dice que $k|(-k'y)$. Ahora como $\text{mcd}\,(k,k')=1$, entonces por el corolario 2.5, $k|(-y)$. Por tanto $y=-\frac{a}{d}t$ y $x=\frac{b}{d}t$, $t\in\mathbb{Z}$.

Teorema 2.13

Sea $d=\text{mcd}(a,b)$. Si la ecuación diofántica lineal $ax+by=c$ tiene una solución $x=x_0$, $y=y_0$, entonces la solución general es $x=x_0+\frac{b}{d}t$, $y=y_0-\frac{a}{d}t$ con $t\in\mathbb{Z}$.

Prueba: Sean $x=x_0$, $y=y_0$, solución de $ax+by=c$. Tenemos,

$$\begin{cases} ax+by=c \\ ax_0+by_0=c \end{cases} \implies \overbrace{a(x-x_0)+b(y-y_0)=0}^{\text{Ecuación homogénea}} \implies \begin{cases} x-x_0=(b/d)\,t \implies x=x_0+(b/d)t \\ y-y_0=(-a/d)\,t \implies y=y_0-(a/d)t \end{cases}$$

Ejemplo 2.26

Consideremos la ecuación en enteros $2x+3y=2$. Como una solución particular es $(x_0,y_0)=(1,0)$, entonces la solución general es $x=1+3t$, $y=0-2t$, $t\in\mathbb{Z}$.

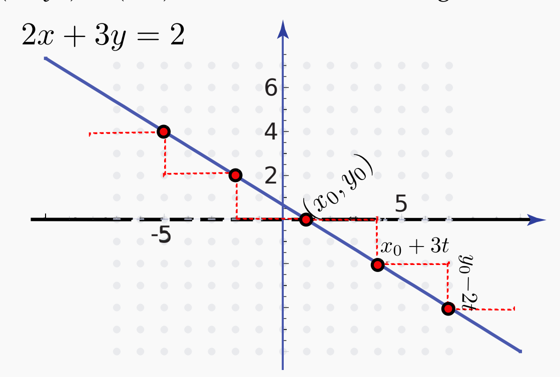


Figura 2.2. Soluciones enteras de la ecuación $2x+3y=2$.

k	x	y
·s		
-4	-11	8
-3	-8	6
-2	-5	4
-1	-2	2
0	1	0
1	4	-2
2	7	-4
3	10	-6
4	13	-8
·s		

2.8 Teorema fundamental de la aritmética

Antes de enunciar el teorema fundamental de la aritmética, veamos un ejemplo muy familiar

Ejemplo 2.27

Podemos factorizar 36 como un producto de primos: En cada paso buscamos el divisor primo más pequeño:

$$\begin{aligned} 36 &= 2\cdot 18 \\ &= 2\cdot 2\cdot 9 \\ &= 2\cdot 2\cdot 3\cdot 3 \end{aligned}$$

El método que usamos es el procedimiento usual de la escuela. Obtener la factorización prima de un número n dividiendo por los primos $\leq n$

36	
18	2
9	2
3	3
1	3

$36=2^2\cdot 3^2$

84	
42	2
21	2
7	3
1	7

$84=2^2\cdot 3\cdot 7$

Lema 2.2 (Lema de Euclides).

Si p es primo y $p|ab$ entonces $p|a$ o $p|b$.

Prueba: Supongamos que $p|ab$ pero $p \nmid a$. En este caso $\operatorname{mcd}(p,a) = 1$ por ser p primo (el único factor en común sería p o 1), entonces por el corolario 2.5, concluimos que $p|b$.

Teorema 2.14 (Fundamental de la aritmética).

Todo número natural compuesto $n > 1$ se puede factorizar de manera única como

$$n = p_1^{\beta_1} p_2^{\beta_2} \cdot s p_k^{\beta_k}$$

donde $p_1, \ldots, p_n$ son primos distintos y $\beta_1, \ldots, \beta_n$ son enteros positivos. Esta factorización se llama *la factorización prima* de n.

Prueba: La prueba se hace por inducción completa. El resultado es cierto para $n = 2$. Supongamos ahora que el resultado es cierto para $n = 3,4,...,k$. Hay que probar que es cierto para $k+1$. Si $k+1$ es primo, listo. Si $k+1$ es compuesto, entonces existen $a,b \in \mathbb{Z}$, $1 < a \leq b < k+1$, tal que $k+1 = ab$. Pero, por hipótesis de inducción a y b factorizan como producto de primos, así que $k+1$ también factoriza como producto de primos, a saber, los factores de a y b.

Unicidad: La prueba es por contradicción. Supongamos que $n = r_1 r_2 \cdot s r_u = q_1 q_2 \cdot s q_v$ donde todos los r_i's y los q_j's son primos, $r_1 \leq r_2 \leq ... \leq r_u$ y $q_1 \leq q_2 \leq ... \leq q_v$. Si cancelamos los primos iguales que hay en ambos lados nos queda

$$r_{i_1} r_{i_2} \cdot s r_{i_n} = q_{j_1} q_{j_2} \cdot s q_{j_m} \quad \text{(todos distintos)}$$

entonces

$$r_{i_1} (r_{i_2} \cdot s r_{i_n}) = q_{j_1} q_{j_2} \cdot s q_{j_m},$$

es decir, r_{i_1} divide a $q_{j_1} q_{j_2} \cdot s q_{i_m}$, entonces por el lema de Euclides, r_{i_1} divide a algún q_{j_t}, por tanto $r_{i_1} = q_{j_t}$: Contradicción pues los asumimos distintos.

Nota: Observe que el número 1 no es ni primo ni compuesto. Esto garantiza la unicidad de la factorización.

Máximo común divisor y Mínimo común Múltiplo.

Definición 2.4

Si $a,b \in \mathbb{Z}^+$ entonces el *mínimo común múltiplo* de a y b es el más pequeño entero $m > 0$ tal que $a|m$ y $b|m$. Se escribe $\operatorname{mcm}(a,b) = m$

Para el teorema que sigue necesitamos aclarar la notación. Necesitamos que dos números tengan los mismos factores primos en una factorización por conveniencia; lo que hacemos es que completamos con potencias p_k^0. Por ejemplo, si

$$a = 2^2 \cdot 3^3 \cdot 7^4 \cdot 19^2$$

$$b = 2 \cdot 3^2 \cdot 11^2,$$

entonces la factorización por conveniencia sería

$$a = 2^2 \cdot 3^3 \cdot 7^4 \cdot \cdot 11^0 \cdot 19^2$$

$$b = 2 \cdot 3^2 \cdot 7^0 \cdot 11^2 \cdot 19^0.$$

Teorema 2.15

Si a,b son enteros positivos, supongamos que

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad \alpha_i \geq 0$$

$$b = \prod_{i=1}^{k} p_i^{\beta_i}, \quad \beta_i \geq 0$$

Donde α_i y β_i podrían ser cero con el propósito de completar la factorización prima de a con los primos de la factorización prima de b y viceversa (se completan con potencias p_k^0). Entonces,

$$\text{mcd}\,(a,b) = \prod_{i=1}^{k} p_i^{\gamma_i}, \quad \gamma_i = \text{mín}\,\{\alpha_i, \beta_i\}, \;\; i = 1,...,k$$

$$\text{mcm}\,(a,b) = \prod_{i=1}^{k} p_i^{\delta_i}, \quad \delta_i = \text{máx}\{\alpha_i, \beta_i\}, \;\; i = 1,...,k$$

En particular $\text{mcd}\,(a,b)\,\text{mcm}\,(a,b) = ab$, es decir

$$\text{mcm}\,(a,b) = \frac{ab}{\text{mcd}\,(a,b)}.$$

Prueba: Ejercicio.

Aunque para números pequeños, el método de la factorización prima sirve para calcular $\text{mcd}\,(n,m)$ y el $\text{mcm}\,(n,m)$, en general, es computacionalmente ineficiente, por el costo de obtener esta factorización. Un algoritmo más adecuado está basado en el teorema (2.5).

Ejemplo 2.28

A partir de la factorización prima de dos números a,b podemos calcular el $\text{mcd}\,(a,b)$ y el $\text{mcm}\,(a,b)$.

36	
18	2
9	2
3	3
1	3

$36 = 2^2 \cdot 3^2 \cdot 7^0$

84	
42	2
21	2
7	3
1	7

$84 = 2^2 \cdot 3 \cdot 7$

Luego, $\text{mcd}(36,84) = 2^2 \cdot 3 \cdot 7^0 = 12$ y el $\text{mcm}(36,84) = 2^2 \cdot 3^2 \cdot 7 = 252.$

Ejemplo 2.29 (Suma de fracciones).

Realizar la suma $\dfrac{5}{36} + \dfrac{7}{84} + \dfrac{3}{4}$.

Solución: Como $\text{mcm}(36,84,4) = 252,$ entonces

$$\begin{aligned}\frac{5}{36} + \frac{7}{84} + \frac{3}{4} &= \frac{7 \cdot 5}{252} + \frac{3 \cdot 7}{252} + \frac{63 \cdot 3}{252} \\ &= \\ &= \frac{245}{252} = \frac{35}{36}\end{aligned}$$

Para el mínimo común múltiplo de una lista de números tenemos un teorema similar al teorema del máximo común divisor.

Teorema 2.16

$\text{mcm}(a_1, a_2, ..., a_n) = \text{mcm}(a_1, \text{mcm}(a_2, ..., a_n)).$

Prueba: Ejercicio.

En la sección que trata sobre el "teorema chino del resto" vamos a necesitar los dos corolarios que siguen y, en su momento, haremos referencia a ellos.

Corolario 2.6 *Si* $m_1, m_2, ..., m_k$ *son primos relativos dos a dos, entonces*

$$\text{mcm}(m_1, m_2, ..., m_k) = m_1 \cdot m_2 \cdot sm_k.$$

Prueba: Ejercicio.

Corolario 2.7 *Si* $m_1, m_2, ..., m_k$, $a \in \mathbb{Z}^+$ *y si* $m_i | a$, $i = 1, 2, ..., k$; *entonces*

$$\text{mcm}(m_1, m_2, ..., m_k) | a.$$

Prueba: Por inducción completa.

La afirmación es claramente correcta para $k=1$ y $k=2$. Asumamos que es correcta para $1,2,...,t$. Ahora, supongamos que $m_i|a, i=1,2,\ldots,t,t+1$ entonces $\operatorname{mcd}(m_1,m_2,\ldots,m_t)|a$ por la hipótesis de inducción y $m_{t+1}|a$, pero entonces los dos números $\operatorname{mcd}(m_1,m_2,\ldots,m_t)$ y m_{t+1} dividen a, así que la hipótesis de inducción nos dice que $\operatorname{mcd}(\operatorname{mcd}(m_1,m_2,\ldots,m_t),m_{t+1})|a$, i.e. $\operatorname{mcm}(m_1,m_2,...,m_k)|a$ por el teorema (2.16).

Ejemplo 2.30

El entero 290290 es divisible por 10, 77, y 13. Como $\operatorname{mcd}(10,77)=1$, $\operatorname{mcd}(10,13)=1$ y $\operatorname{mcd}(77,13)=1$; entonces $\operatorname{mcm}(10,77,13)=10\cdot 77\cdot 13=10010$ y $10010\,|\,290290$.

Ejemplo 2.31

Muestre que si $p=4k+1$ y $p=3k'+1$ entonces hay un $k''\in\mathbb{Z}$ tal que $p=12k''+1$

Solución: Como $\operatorname{mcd}(4,3)=1$, $4|(p-1)$ y $3|(p-1)$, entonces $\operatorname{mcm}(3,4)=12$ y $12|(p-1)$, es decir, hay un $k''\in\mathbb{Z}$ tal que $p-1=12k''$.

EJERCICIOS

2.8 Muestre que los divisores de n ocurren en pares, es decir, si $d|n$ con $n=kd$, entonces $k|n$.

2.9 De un par de ejemplos que muestren que en general, si $d=\operatorname{mcd}(a,b)$, entonces $d\neq\operatorname{mcd}(a,a-nb)$ con $n\in\mathbb{Z}$

2.10 Muestre que $\operatorname{mcd}(ab,m)\,|\operatorname{mcd}(a,m)\operatorname{mcd}(b,m)$ (Use Id. Bezout).

2.11 Muestre que $\operatorname{mcd}(a,b)=1$ entonces $\operatorname{mcd}(a,m)\operatorname{mcd}(b,m)=\operatorname{mcd}(ab,m)$

2.12 Probar el corolario 2.4.

2.13 Muestre que si $\operatorname{mcd}(a,b)=1$ y si $\operatorname{mcd}(a,c)=1$,

2.14 Muestre que si $\operatorname{mcd}(a_1,m)=1, \operatorname{mcd}(a_2,m)=1,\;\ldots\;, \operatorname{mcd}(a_k,m)=1$ entonces $\operatorname{mcd}(a_1\cdot a_2\cdot sa_k,\; m)=1$.

2.15 Muestre, usando la identidad de Bezout, que si $\operatorname{mcd}(a,b)=d$ y si $a=k_1d$ y $b=k_2d$, entonces $\operatorname{mcd}(k_1,k_2)=1$

2.16 Muestre que si $d=\operatorname{mcd}(a,b)$ y si $ra+sb=d$, entonces $\operatorname{mcd}(r,s)=1$.

2.17 Muestre que si $am+bn=h$ entonces $\operatorname{mcd}(a,b)|h$

2.18 Muestre que la ecuación diofántica $ax + by = h$ tiene solución solo si $\operatorname{mcd}(a,b)|h$

2.19 Resuelva la ecuación diofántica $24 = 365x + 1876y$

2.20 Sea p un número primo. Determinar todos los enteros$k \in \mathbb{Z}$ tales que $\sqrt{k^2 - kp}$ es natural. **Ayuda:** Si $p^2 = ab \implies (a = p \wedge b = p) \vee (a = p^2 \wedge b = 1)$

2.21 Sean $q_1, \ldots, q_n$ y p_i todos números primos distintos. Use inducción matemática para probar que si $p_i | q_1 q_2 \cdot s q_n$ entonces $p_i = q_j$ para algún $j \in 1,2,...,n$.

2.22 Sea p primo, si $p|a^n \implies p|a$

2.23 Muestre que si p es primo, entonces $\sqrt[n]{p}$ no es racional. **Ayuda:** Por contradicción, suponga $\sqrt[n]{p} = a/b$ con $\operatorname{mcd}(a,b) = 1$.

2.24 Sean $\operatorname{mcd}(a,b) = 1$ y p primo, entonces $p \nmid \operatorname{mcd}(a^n, b^n)$.

2.25 Muestre que si $\operatorname{mcd}(a,p) = 1$ con p primo, entonces $\operatorname{mcd}(a,p^s) = 1$, con $s > 0$.

2.26 Sean m y n son primos relativos. Muestre que si $mn = a^k$, $k \geq 0$; entonces existe $x,y \in \mathbb{Z}$ tal que $m = x^k$ y $n = y^k$. **Ayuda:** Use la descomposición en factores primos de cada uno de los números.

2.27 Consideremos la descomposición prima $n = \prod_i^k p_i^{\alpha_i}$. ¿$\operatorname{mcm}(p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}) = n$?

2.28 Supongamos que los enteros m y n son primos relativos. Muestre que si $d|mn$, entonces $\exists b,c$ únicos tal que $d = bc$ con $b|m$ y $c|n$.

2.29 Si $4|p-3$ y $3|p-1$, muestre que $12|p+1$.

2.30 Sea $n > 1$ y p el más pequeño divisor primo de n. Muestre que $\operatorname{mcd}(n, p-1) = 1$

2.31 Encuentre tres números a,b,c tal que $\operatorname{mcd}(a,b,c) = 1$ pero que $\operatorname{mcd}(a,b) \neq 1$, $\operatorname{mcd}(a,c) \neq 1$, $\operatorname{mcd}(b,c) \neq 1$.

2.32 Probar que dos enteros consecutivos son primos relativos

2.33 Probar que si $\operatorname{mcd}(a,b) = \operatorname{mcm}(a,b) \Longrightarrow a = b$.

2.34 Muestre que $\operatorname{mcd}(mg, g) = g$ si $g \in \mathbb{N}$.

2.35 Si $a,b \in \mathbb{N}$, y si $a|b$ calcule $\operatorname{mcd}(a,b)$ y $\operatorname{mcm}(a,b)$.

2.36 Muestre que $(\exists x, y \in \mathbb{Z}$ tal que $x + y = s \wedge \operatorname{mcd}(x,y) = g) \iff g|s, g \in \mathbb{Z}^+$ **Ayuda:** Una implicación es directa por Bezout, la otra requiere descomponer $kg = (k-1)g + g$

2.37 Mostrar que si $\text{mcd}(a,b) = \text{mcd}(c,d) = 1$ y si $\frac{a}{b} + \frac{c}{d} \in \mathbb{Z}$ entonces $|b| = |d|$. **Ayuda:** Si $p|qc$ y $\text{mcd}(p,q) = 1$, entonces $p|c$.

2.38 Mostrar que $\text{mcd}(a,\, b) = \text{mcd}(a,\, b,\, ax + by)$ con $x,y \in \mathbb{Z}$

2.39 Muestre que $\text{mcd}(a, a+2) = 1$ ó 2

2.40 Sea p_i el $i-$ésimo primo y sea $N = p_1 p_2 \cdot s p_{n-1} + 1$. Muestre que $N \geq p_n$.

2.41 Sean $m,a,b \in \mathbb{Z}$. Muestre que $\text{mcd}(ma, mb) = |m|\,\text{mcd}(a,b)$

2.42 Sea $\text{mcd}(a,b) = 1$. Muestre que si $d = \text{mcd}(a+b, a-b)$ entonces $d = 1$ o $d = 2$.
Sea $\text{mcd}(a,b) = 1$ y $d = \text{mcd}(a+2b, 2a+b)$. Muestre que $d|3a$ y $d|3b$ y por tanto, $d = 1$ o $d = 3$.

2.43 Muestre que para todo $n \in \mathbb{N}$, $n > 1$; $A = 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n}$ *no* es entero

2.44 Mostrar que si $d|(n^2+1)$ y $d|((n+1)^2+1)$ para algún entero n, entonces $d = 1$ $d = 5$.

2.45 Probar que la fracción $(21n+4)/(14n+3)$ es irreducible para cualquier $n \in \mathbb{Z}$

2.46 Sea $N = 2^p - 1$,

a) Probar que $2^{ab} - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + 2^{3a} + \cdot s + 2^{(b-1)a})$. **Ayuda:** Usar la identidad $1 + x + x^2 + x^3 + \cdot s + x^k = \frac{1 - x^{k+1}}{1 - x}$, $x \neq 1$, $k \in \mathbb{N}$.

b) Muestre que si N es primo, entonces p es primo.

2.47 Considere los números de Euler: $T_n = 2^{2^n} + 1$ con $n \in \mathbb{N}$.

a) Muestre que $2^{2^n} - 1 = T_{n-1}^2 - 2T_{n-1}$

b) Muestre, usando a), que $T_n - 2 = T_{n-1} T_{n-2} \cdot s T_0$

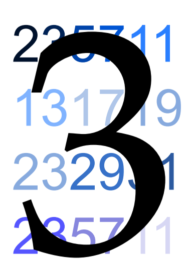
c) Muestre que si $m > n$, $\text{mcd}(T_n, T_m) = 1$

2.48 Sea n entero positivo y S un conjunto con $n+1$ elementos distintos tomados del conjunto $\{1,2,...,2n\}$. Muestre que hay al menos dos elementos en S primos relativos

2.49 $n \geq 2$. Supongamos que tomamos $n+1$ enteros al azar. Muestre que hay dos elementos tal que su diferencia es divisible por n. **Ayuda:** usar le principio del palomar y el algoritmo de la división: $n+1$ enteros producen $n+1$ restos, pero dividir por n solo produce n restos...

2.50 Mostrar que hay un número infinito de primos de la forma $4n+3$.
Ayuda: Asuma que solo hay k primos de esa forma y considere el número $N = 4p_1 p_2 \cdot s p_k + 3$.





CONGRUENCIAS

3.1 Congruencias módulo m

Recordemos que estabamos usando '$r = \text{rem}(a,m)$' para indicar el resto (en el teorema de la división) de dividir a por m. Dos números *"son congruentes módulo m"* si dejan el mismo residuo al dividir por m, es decir si $\text{rem}(a,m) = \text{rem}(b,m)$. Como $a = qm + \text{rem}(a,m)$ y $b = q'm + \text{rem}(b,m)$ entonces $m|(b-a)$.

Todos los números son congruentes módulo $m = 1$. Si usamos $m = 2$, los pares son congruentes con los pares (resto 0 módulo 2) y los impares con los impares (resto 1 módulo 2). En general, la idea es 'agrupar' los números según el residuo que dejan al dividir por m. Estos subconjuntos constituyen una partición de $\mathbb{Z}$ de tal manera que podemos trabajar no con todo $\mathbb{Z}$ sino con un grupo de representantes.

Definición 3.1

Sea $m \in \mathbb{Z}$, $m \geq 1$. Decimos que a es congruente con b módulo m si $m|(b-a)$. Escribimos

$$a \equiv b \pmod{m} \quad \text{o también} \quad a \equiv_m b$$

Ejemplo 3.1

a.) $10 \equiv 0 \pmod 5$ pues $5|(10-0)$

b.) $10 \equiv 1 \pmod 3$ pues $3|(10-1)$

c.) $10 \equiv -1 \pmod{11}$ pues $11|(10+1)$

d.) $5 \equiv 3 \pmod 2$ pues $2|(3-5)$

Teorema 3.1

$a \equiv b \pmod m \iff$

(i) $b - a \equiv 0 \pmod m$

(ii) $a = mk + b$, para algún $k \in \mathbb{Z}$

(iii) $\text{rem}(a,m) = \text{rem}(b,m)$ (residuos módulo m)

Prueba: Probemos (iii) usando el teorema de la división.

$'' \Longrightarrow ''$ Sea $\text{rem}(a,m) = r_1$ y $\text{rem}(b,m) = r_2$, es decir, $a = q_1 m + r_1$ con $0 \leq r_1 < m$ y $b = q_2 m + r_2$ con $0 \leq r_2 < m$. Supongamos que $r_1 > r_2$, entonces $b - a = (q_1 - q_2)m + (r_1 - r_2)$ con $0 \leq r_1 - r_2 < m$ pues $0 < r_1 - r_2 < r_1 < m$. Pero $m|(b-a)$, por tanto $b - a = mq_3$, como el resto es único (en el esquema del teorema de la divisón) entonces $r_2 = r_1$. El caso $r_1 < r_2$ es idéntico.

$'' \Longleftarrow ''$ Si $a = q_1 m + r_1$ con $0 \leq r_1 < m$ y $b = q_2 m + r_2$ con $0 \leq r_2 < m$, entonces $b - a = q_3 m$, es decir, $m|(b-a)$.

(Notación de congruencia y residuo).

Si r es el residuo $r = \text{rem}(a,m)$, entonces $a \equiv r \pmod{m}$

El símbolo "$\equiv$" se puede manipular como "$=$" excepto para la cancelación:

Teorema 3.2

Sean $a \equiv b \pmod{m}$ $a' \equiv b' \pmod{m}$ y $c,k \in \mathbb{Z}$. Entonces,

a.) $ka \equiv kb \pmod{m}$, en particular si $k \geq 0$, $a^k \equiv b^k \pmod{m}$.

b.) $aa' \equiv bb' \pmod{m}$

c.) $a \pm a' \equiv b \pm b' \pmod{m}$

d.) $a \equiv a \pmod{m}$ para toda $a \in \mathbb{Z}$

e.) $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$

f.) $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$

g.) Sea $a \neq 0$, $ab \equiv ac \pmod{m} \wedge \text{mcd}\,(a,m) = d \Longrightarrow b \equiv c \pmod{\frac{m}{d}}$

h.) Sea $a \neq 0$, $ab \equiv ac \pmod{m} \wedge \text{mcd}\,(a,m) = 1 \Longrightarrow b \equiv c \pmod{m}$

i.) Si $a \equiv b \pmod{m}$ y $d|m$, entonces $a \equiv b \pmod{d}$

Prueba: Sólo vamos a probar algunos items, el resto queda como ejercicio.

b.) $aa' \equiv bb' \pmod{m}$: Por hipótesis existen $k,k' \in \mathbb{Z}$ tal que $b = mk + a$ y $b' = mk' + a'$, multiplicando obtenemos $bb' = m(mkk' + ka' + k'a) + aa' \Longrightarrow m|(bb' - aa')$.

g.) $ab \equiv ac \pmod{m} \wedge \text{mcd}\,(a,m) = d \Longrightarrow b \equiv c \pmod{\frac{m}{d}}$: En efecto, como $d = \text{mcd}\,(a,m)$ entonces $\frac{a}{d}$ y $\frac{m}{d}$ son enteros y $\text{mcd}\left(\frac{a}{d}, \frac{m}{d}\right) = 1$.
Por hipótesis, existen $k \in \mathbb{Z}$ tal que $ac - ab = mk \Longrightarrow a(c-b) = mk \Longrightarrow \frac{a}{d}(c-b) = \frac{m}{d}k$.
Así, $\frac{m}{d}\left|\frac{a}{d}(c-b)\right. \wedge \text{mcd}\left(\frac{a}{d}, \frac{m}{d}\right) = 1 \Longrightarrow \frac{m}{d}|(c-b)$ por el corolario **??**.

Ejemplo 3.2 (Manipulación algebraica módulo m).

a.) Muestre que si $a \equiv b \pmod m$ y si $c \equiv a + d \pmod m$ entonces $c \equiv b + d \pmod m$.

Solución: Como $0 \equiv b - a \pmod m$ y $c \equiv a + d \pmod m$, sumando miembro a miembro (teorema 3.2 **c.)**) se obtiene $c \equiv b + d \pmod m$

b.) Muestre que si $a \equiv b \pmod m$ y si $c \equiv ad \pmod m$ entonces $c \equiv bd \pmod m$

Solución: Existe $k, k' \in \mathbb{Z}$ tal que $a = mk + b$ y $c - ad = mk'$, entonces $c - ad = c - (mk + b)d = mk' \implies c - bd = m(k' + kd) \implies c \equiv bd \pmod m$.

c.) $d \equiv [\overbrace{8+2}^{\equiv_{10} 0} + \overbrace{3+2+5}^{\equiv_{10} 0} + \overbrace{5+2}^{\equiv_{10} 7}] \pmod{10} \implies d \equiv 7 \pmod{10}$

d.) Calcular $\text{rem}(9^5, 5)$ (el resto de dividir 9^5 por 5).

Solución: Recordemos que $\text{rem}(9^5, 5) = r$ si $9^5 \equiv r \pmod 5$. Como $9 \equiv -1 \pmod 5$ entonces $9^5 \equiv (-1)^5 \pmod 5$, es decir $\text{rem}(9^5, 5) = -1$ o también $9^5 = 11810 \cdot 5 - 1$.

Si queremos el resto positivo (como en el esquema del teorema de la división), observamos que $-1 \equiv 4 \pmod 5$, por tanto $\text{rem}(9^5, 5) = 4$ o también $9^5 = 11809 \cdot 5 + 4$.

Ejemplo 3.3

Calcular el resto de dividir 15^{196} por 13.

Solución: La idea es descomponer 15^{196} en potencias más pequeñas. Si r es el resto buscado, $15^{196} \equiv r \pmod{13}$.

$$\begin{array}{lcll}
15^{196} & \equiv & \text{rem}(2^{196}, 13), & \text{pues } 15 \equiv 2 \pmod{13}, \\
 & \equiv & \text{rem}((2^{2\cdot 2})^{7\cdot 7}, 13), & \text{pues } 196 = 2\cdot 2\cdot 7\cdot 7, \\
 & \equiv & \text{rem}((3^7)^7, 13), & \text{pues } 2^4 = 16 \equiv 3 \pmod{13}, \\
 & \equiv & \text{rem}((3)^7, 13), & \text{pues } 3^7 = (3^3)^2 \cdot 3 \equiv_{13} 1^2 \cdot 3 \equiv 3 \pmod{13} \\
 & \equiv & \text{rem}(3, 13) & \text{pues } 3^7 \equiv 3 \pmod{13}.
\end{array}$$

Así, el resto de dividir 15^{196} por 13 es 3.

Ejemplo 3.4

Resolver $4x \equiv 8 \pmod{12}$ con $x \in \{0, 1, 2, ..., 11\}$.

Solución: Podríamos resolver esta congruencia por ensayo y error, pero la vamos a resolver usando el teorema 3.2 **g.)**.

$4x \equiv 8 \pmod{12} \implies x \equiv 2 \pmod 3$ por el teorema 3.2 **g.)**

Luego, los $x \in \{0,1,2,...,11\}$ que dejan resto 2 al dividir por 3 son $x = 2,5,8$ y 11.

No siempre usamos el residuo del teorema de la divisón porque a veces los residuos negativos son, en valor absoluto, más pequeños.

Ejemplo 3.5

Calcular el resto de la división de 12^{201} por 13, es decir, calcular $12^{201} \bmod 13$

Como $12 \equiv -1 \pmod{13} \implies 12^{201} \equiv (-1)^{201} \pmod{13}$. Entonces, por transitividad $12^{201} \equiv 12 \pmod{13}$. Esto dice que $12^{201} \bmod 13 = 12 \bmod 13 = 12$

Ejemplo 3.6

Calcular $13^{300} \bmod 7$.

Aunque $13 \equiv 5 \pmod 7$ es mejor iniciar con $13 \equiv -2 \pmod 7$ pues de esta congruencia obtene-mos $13^3 \equiv -8 \pmod 7$ y $-8 \equiv 1 \pmod 7$. Así, $13^{300} \equiv 1 \pmod 7 \implies$ $13^{300} \bmod 7 = 1 \bmod 7 = 1$.

3.2 (*) Calendarios: ¿Qué día nació Ud?.

Supongamos que queremos saber el día de la semana correspondiente a una fecha dada: Por ejemplo, ¿qué día fue el 9 de mayo de 1973?

En varios libros se hace un análisis de como resolver este problema, por ejemplo en [3]; aquí solo vamos a dar la solución, según el calendario Gregoriano.

Primero debemos numerar los días y los meses, como se muestra en en la tabla que sigue (a febrero se le asigna el 12; febrero es especial por ser el mes al que se agrega un día en año bisiesto).

Ahora, sea $f =$ fecha, $m =$ mes, $a =$ año, $s =$ siglo y $n =$ años en el siglo. Por ejemplo, si tenemos la fecha: abril 1, 1673 entonces: $f = 1$, $m = 2$, $a = 1673 = 100s + n$ donde $s = 16$ y $n = 73$.

Finalmente, si d denota el día de la semana correspondiente a la fecha (f,m,a), entonces

Domingo	= 0	Marzo	= 1	Octubre	= 8
Lunes	= 1	Abril	= 2	Noviembre	= 9
Martes	= 2	Mayo	= 3	Diciembre	= 10
Miércoles	= 3	Junio	= 4	Enero	= 11
Jueves	= 4	Julio	= 5	Febrero	= 12
Viernes	= 5	Agosto	= 6		
Sábado	= 6	Setiembre	= 7		

Tabla 3.1

$$d \equiv f + \left[\!\left[\frac{13m-1}{5}\right]\!\right] - 2s + n + \left[\!\left[\frac{s}{4}\right]\!\right] + \left[\!\left[\frac{n}{4}\right]\!\right] \pmod 7$$

Un detalle. En esta redistribución, el año inicia en Marzo y finaliza en Febrero. Este es un detalle a tener en cuenta: *Las fechas que involucran a enero y febrero se les debe restar un año*, pues en esta fórmula estos meses están en el año anterior. Por ejemplo, si tenemos la fecha 3 de enero del 2010 entonces $f = 3$, $m = 11$ y $a = 2009 = 100s + n$ donde $s = 20$ y $n = 9$.

		$100s+n$			
$100s+n-1$		marzo	abril	$\cdots$	diciembre
enero	febrero	marzo	abril	$\cdots$	diciembre

Ahora ya puede calcular qué día nació Ud.

Ejemplo 3.7

a.) El 9 de mayo de 1973 fue *miércoles = 3;* pues $f = 9$, $m = 3$, $A = 1973 = 100s + n$ con $s = 19$ y $n = 73$. Usando la fórmula obtenemos,

$$d \equiv 9 + 7 - 38 + 73 + 4 + 18 \equiv 3 \pmod 7$$

a.) El 3 de enero del 2010 fue *domingo = 0;* pues $f = 3$, $m = 11$, $A = 2009 = 100s + n$ con $s = 20$ y $n = 9$. Usando la fórmula obtenemos,

$$d \equiv 3 + 28 - 40 + 19 + 5 + 4 \equiv 0 \pmod 7$$

a.) El 29 de febrero del 2008 fue viernes, verifíquelo!

Implementación en Excel.

[Descargar]

	A	B	C	D	E	F	G
1	**Qué día nació usted?**			Domingo = 0	Marzo = 1	Octubre = 8	
2	Ejemplo: 1 de abril 1978			Lunes = 1	Abril = 2	Noviembre = 9	
3				Martes = 2	Mayo = 3	Diciembre = 10	
4				Miércoles = 3	Junio = 4	Enero = 11	
5				Jueves = 4	Julio = 5	Febrero = 12	
6				Viernes = 5	Agosto = 6		
7	f	m	s	Sábado = 6 n	Setiembre = 7 Calcular día		
8	1	2	19	78	6		

```
Private Sub CommandButton1_Click()
Dim f, m, s, n, d, dia
 f = Cells(8, 1)
 m = Cells(8, 2)
 s = Cells(8, 3)
 n = Cells(8, 4)
 If m=11 or m=12 then
    n=n-1
 End If
d = (f+Int((13*m-1)/5)-2*s+n+Int(s/4)+Int(n/4))Mod 7
If d<0 then
   d=d+7
End If
 dia = Switch(d = 0,"D",d =1,"L",d=2,"K",d=3,"M",d=4,"J",d=5,"V",d=6,"S")
 Cells(8, 5) = dia
End Sub
```

3.3 Trucos de divisibilidad.

Si $a = a_n 10^n + a_{n-1}10^{n-1} + ... + a_1 10 + a_0$, la suma de sus dígitos es congruente con a módulo 9, en efecto, como $10 \equiv 1 \pmod 9$ entonces $10^i \equiv 1 \pmod 9, i = 0,1,2,...$ Luego, multiplicando por a^i y sumando

$$\sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \pmod 9 \implies a \equiv \sum_{i=0}^{n} a_i \pmod 9$$

$$\sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i \pmod 3 \implies a \equiv \sum_{i=0}^{n} a_i \pmod 3 \quad \text{pues} \quad 3|9$$

a.) **Divisibilidad por** $9:$ 9 divide a a si y sólo si 9 divide la suma de sus dígitos, es decir, $9|a \iff 9\,|\sum_{i=0}^{n} a_i$

En efecto, como $a \equiv \sum_{i=0}^{n} a_i \pmod 9$ entonces $9 \,|\, (\sum_{i=0}^{n} a_i - a)$. Si $9|a$ entonces divide la suma de sus dígitos y si 9 divide la suma de los dígitos de a entonces divide a a.

b.) **Divisibilidad por** 3 **:** 3 divide a a si y sólo si 3 divide la suma de sus dígitos. La demostración es igual a la anterior, cambiando 9 poe 3.

c.) **Divisibilidad por** 2 y por 5 **:** tanto 2 como 5 dividen a a si y sólo si dividen a_0.

En efecto: Observemos que $a = \sum_{i=1}^{n} a_i 10^i + a_0$. Tanto 2 como 5 dividen a $a_i 10^i$, por tanto, dividen a la suma $\sum_{i=1}^{n} a_i 10^i + a_0$ si y solo si tanto 2 y 5 dividen a a_0

d.) **Divisibilidad por** 11 **:** 11 divide a a si y sólo si 11 divide la suma alternada de sus dígitos, es decir, $11 \,|\, \sum_{i=0}^{n} (-1)^i a_i$

En efecto, esto es consecuencia de que $10 \equiv -1 \pmod{11}$.

3.4 (*) Cuadrados Mágicos

Un cuadrado mágico es un arreglo de $n \times n$ números en el que la suma de las entradas de cada fila o columna siempre es la misma. Por ejemplo, consideremos el cuadrado mágico 3×3

$$\begin{bmatrix} 4 & 2 & 6 \\ 0 & 7 & 5 \\ 8 & 3 & 1 \end{bmatrix}, \quad \text{tanto las filas como las columnas suman } 12$$

En la actualidad hay varios métodos para construir cuadrados mágicos. En 1693 De la Loubère dio un método para construir cuadrados mágicos para cualquier n impar, el método es llamado el "Método Siamés". En 1929 D.N. Lehmer investigó, por medio de congruencias, una generalización de este método. El resultado es una manera sencilla de colocar los números $0, 1, \ldots, n^2 - 1$ en un arreglo $n \times n$ de tal manera que sea un cuadrado mágico. Este método, llamado método del "paso uniforme", calcula la entrada (i, j), usando congruencias, en la que se debe colocar cada uno de los números $k = 0, 1, \ldots, n^2 - 1$ para que el arreglo resulte "mágico".



Albrecht Dürer, "Melencolia I"

Definición 3.2

Supongamos que n^2 enteros diferentes son colocados en un arreglo $n \times n$. Si la suma de las entradas de cada fila suma siempre lo mismo, decimos que el cuadrado es "mágico por filas". Si la suma de las entradas de cada columna suma siempre lo mismo, decimos que el cuadrado es "mágico por columnas". Si el cuadrado es ambos "mágico por filas" y "mágico por columnas", se dice "cuadrado mágico" y la suma se dice "suma mágica".

Teorema 3.3

Sea n entero positivo impar y a,b,c,d,e,f enteros, tal que $\text{mcd}(cf-de,n)=1$ Sea $A=(a_{ij})$ la matriz $n\times n$ definida así: Para cada $k=0,1,...,n^2-1,$

$$a_{i+1,j+1}=k \quad \text{si} \quad i\equiv a+c\cdot k+e\cdot [\![k/n]\!] \pmod n \quad \text{y} \quad j\equiv b+d\cdot k+f\cdot [\![k/n]\!] \pmod n$$

Entonces,
Si $\text{mcd}(c,n)=\text{mcd}(e,n)=1$, el cuadrado es "mágico por columnas".
Si $\text{mcd}(d,n)=\text{mcd}(f,n)=1$, el cuadrado es "mágico por filas".
Si $\text{mcd}(c,n)=\text{mcd}(d,n)=\text{mcd}(e,n)=\text{mcd}(f,n)=1$, el cuadrado es mágico. En cada caso la suma mágica es $n(n^2-l)/2$.

Ejemplo 3.8

Sea $n=7$ y $a=4$, $b=3$, $c=1$, $d=-2$, $e=1$, $f=-4$. Como $\text{mcd}(c,n)=\text{mcd}(d,n)=\text{mcd}(e,n)=\text{mcd}(f,n)=1$, el método construye un cuadrado mágico 7×7 con suma mágica 168.

$k=0:\ i\equiv 4+1\cdot 0+1\cdot[\![0/7]\!] \pmod 7$ y $j\equiv 3-2\cdot 0-4\cdot[\![0/7]\!] \pmod 7 \Rightarrow a_{5,4}=0$
$k=1:\ i\equiv 4+1\cdot 1+1\cdot[\![1/7]\!] \pmod 7$ y $j\equiv 3-2\cdot 1-4\cdot[\![1/7]\!] \pmod 7 \Rightarrow a_{6,2}=1$
$k=2:\ i\equiv 4+1\cdot 2+1\cdot[\![2/7]\!] \pmod 7$ y $j\equiv 3-2\cdot 2-4\cdot[\![2/7]\!] \pmod 7 \Rightarrow a_{7,7}=2$
...

$$\begin{bmatrix} 15 & 40 & 9 & 34 & 3 & 21 & 46 \\ 10 & 28 & 4 & 22 & 47 & 16 & 41 \\ 5 & 23 & 48 & 17 & 35 & 11 & 29 \\ 42 & 18 & 36 & 12 & 30 & 6 & 24 \\ 37 & 13 & 31 & 0 & 25 & 43 & 19 \\ 32 & 1 & 26 & 44 & 20 & 38 & 7 \\ 27 & 45 & 14 & 39 & 8 & 33 & 2 \end{bmatrix}$$

Implementación usandoMathematica. La implementación, usando Mathematica, es muy sencilla,

```
a = 4; b = 3; c = 1; d = -2; e = 1; f = -4; n = 7;

(*Verificar si son primos relativos?*)
{GCD[c*f - d*e, n], GCD[c, n], GCD[d, n], GCD[e, n], GCD[f, n]}

B = Array[A, {n, n}]; (*A[i,j]=k*)

Do[A[Mod[a + c*k + e*Floor[k/n], n] + 1,
   Mod[b + d*k + f*IntegerPart[k/n], n] + 1] = k, {k, 0, n^2 - 1}
   ]

MatrixForm[B]
```

Implemetnación en VBA Excel.

[Descargar]

	A	B	C	D	E	F	G	H	I	J	K	L
1		Cuadrados mágicos (método Siámes)										
2		Si mcd(cf-de,n)=mcd(c,n)=mcd(d,n)=mcd(e,n)=mcd(f,n)=1, el cuadrado es mágico										
3	n	a	b	c	d	e	f		Cuadrado mágico			
4	7	4	3	1	-2	1	-4					
5												
6		15	40	9	34	3	21	46				
7		10	28	4	22	47	16	41				
8		5	23	48	17	35	11	29				
9		42	18	36	12	30	6	24				
10		37	13	31	0	25	43	19				
11		32	1	26	44	20	38	7				
12		27	45	14	39	8	33	2				
13												

```
Private Sub CommandButton1_Click()
Dim n, a, b, c, d, e, f, k, i, j
Dim CM() 'Matriz=Cuadrado m\'agico
n = Cells(4, 1) : a = Cells(4, 2) : b = Cells(4, 3)
c = Cells(4, 4) : d = Cells(4, 5) : e = Cells(4, 6)
f = Cells(4, 7)
If mcd(c * f - d * e, n) = 1 And mcd(c, n) = 1 And mcd(d, n) = 1
                      And mcd(e, n) = 1 And mcd(f, n) = 1 Then
 ' nada
Else: MsgBox "No se cumplen las condiciones del teorema!!! "
End If

ReDim MC(1 To n, 1 To n)
For k = 0 To n ^ 2 - 1
   i = (a + c * k + e * Int(k / n)) Mod n
   j = (b + d * k + f * Int(k / n)) Mod n
   'Queremos residuos positivos
   If i < 0 Then
      i = i + n
   End If
   If j < 0 Then
      j = j + n
   End If
   MC(i + 1, j + 1) = k
Next k

'Imprimir la matriz
For i = 1 To n
   For j = 1 To n
    Cells(5 + i, 1 + j) = MC(i, j)
   Next j
```

```
Next i

End Sub
Function mcd(a, b)
   Dim c As Long, d As Long, r As Long 'max = 2 147 483 647
      c = Abs(a) : d = Abs(b)
   While d <> 0
      r = c Mod d 'residuo entre (c,d)
      c = d : d = r
   Wend
   mcd = Abs(c)
End Function
```

3.5 Clases residuales módulo m

Sea $m \in \mathbb{Z}$ con $m > 1$. La relación "congruente módulo m", denotada por brevedad con "$\equiv_m$", se define así:

$$a \equiv b \pmod m \iff m|(b-a)$$

La relación "$\equiv_m$" es una relación de equivalencia, es decir, particiona $\mathbb{Z}$ en clases (de equivalencia.) El *conjunto cociente* "$\mathbb{Z}/\equiv_m$", es el conjunto de clases de equivalencia. También se usa la notación $\mathbb{Z}/Zm$ o $\mathbb{Z}_m$. Denotamos con $\overline{a}$ la clase cuyo representante es a, es decir,

$$\text{En } \ \mathbb{Z}_m, \ \ \overline{a} = \{b \in \mathbb{Z} \ : \ a \equiv b \pmod m\}. \ \ \text{En particular, } \ \overline{0} = \overline{m}.$$

Es fácil saber a qué clase pertence un $a \in \mathbb{Z}$ arbitrario: Si $a \in Z$ y $a = mk + r$ con $0 \leq r < m$, entonces $a \equiv r \pmod m$. Entonces es natural tomar como representante de clase los residuos positivos más pequeños, es decir $\overline{a} = \overline{\text{rem}(a,m)}$ (recordemos que " $\text{rem}(a,m)$" denota el más pequeño residuo ≥ 0 de dividir a por m).

Ejemplo 3.9

Si $m = 2$. Al dividir por dos solo hay dos posibilidades: Que el número se a par y el resto es 0 o que el número sea impar y el resto es 1. Por tanto $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, es decir $\mathbb{Z}$ se particiona en dos conjuntos, los pares y los impares.

Ejemplo 3.10

La relación "$\equiv_5$" particiona $\mathbb{Z}$ en 5 clases pues, por el teorema de la división, si $a \in Z$, existe $k \in \mathbb{Z}$ tal que $a = k \cdot 5 + r$ con $0 \leq r < 5$; entonces al dividir por 5 solo hay posibilidad de cinco residuos: 0,1,2,3 o 4.

El conjunto cociente es $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

$\overline{0} = \{5k \,:\, k \in \mathbb{Z}\} = \{0, \pm 5, \pm 10, ...\}$

$\overline{1} = \{5k+1 \,:\, k \in \mathbb{Z}\} = \{..., -9, -4, 1, 6, 11, ...\}$

$\overline{2} = \{5k+2 \,:\, k \in \mathbb{Z}\} = \{..., -8, -3, 2, 7, 12, ...\}$

$\overline{3} = \{5k+3 \,:\, k \in \mathbb{Z}\} = \{..., -7, -2, 3, 8, 13, ...\}$

$\overline{4} = \{5k+4 \,:\, k \in \mathbb{Z}\} = \{..., -6, -1, 4, 9, 14, ...\}$

En este contexto, a las clases de equivalencia se les denomina *clases residuales módulo* m y, como deciamos más arriba, el conjunto cociente se denota con $\mathbb{Z}_m$ (o también $\mathbb{Z}/m\mathbb{Z}$) en vez de $\mathbb{Z}/\equiv_m$.

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \cdots \overline{m-1}\} \;\text{ y }\; \mathbb{Z} = \overline{0} \cup \overline{1} \cup \cdots \cup \overline{m-1}$$

Por abuso del lenguaje, es usual poner

$$\mathbb{Z}_m = \{0,\ 1,\ 2,\ 3, \cdots m-1\}$$

Observe que: Si $n \in \mathbb{Z}$ entonces n debe estar en alguna clase y solo una, de $\mathbb{Z}_m$

Ejemplo 3.11

Muestre que si $p > 3$ es primo, p es de la forma $6k \pm 1$.

Solución: Mmmmmm...Idea: Si $p = 6k \pm 1$ entonces $p \equiv \pm 1 \pmod 6$.

Como $p \in \mathbb{Z}$, p debe estar en alguna de las clases de $\mathbb{Z}_6$. No está en $\overline{0}, \overline{2}$ ni $\overline{4}$ pues estas clases solo contienen pares (sus elementos son números de la forma $6k$, $6k+2$, $6k+4$, respectivamente). No está en $\overline{3}$ pues esta clase solo números de la forma $6k+3$ que son múltiplos de 3. Así que $p \in \overline{1}$ o $p \in \overline{5} = \overline{-1}$. Es decir, p es de la forma $6k \pm 1$.

Permutaciones módulo m. En las aplicaciones a veces se usan otros conjuntos de representantes para las clases.A estas representaciones las llamamos *permutaciones* del conjunto $\{0, 1, 2, ..., m-1\}$ módulo m.

Por ejemplo, $\mathbb{Z}_5 = \{5, 7, 6, -6, 13\}$ es una *permutación módulo* 5 de $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ pues

$$\begin{aligned} 5 &\equiv 0 \pmod 5),\\ 7 &\equiv 2 \pmod 5),\\ 6 &\equiv 1 \pmod 5),\\ -6 &\equiv 4 \pmod 5) \quad \text{y}\\ 13 &\equiv 3 \pmod 5), \end{aligned}$$

Además, por supuesto, $\mathbb{Z}_5 = \{5,7,6,-6,13\} = \{0,1,2,3,4\}$

- Si m es impar, la *representación simétrica* de $\mathbb{Z}_m$ es

$$\left\{-\frac{m-1}{2},\ldots,-1,\,0,\,1,\ldots\frac{m-1}{2}\right\}$$

En efecto,

$$\begin{aligned} 0 &\equiv 0 \pmod m),\\ 1 &\equiv 1 \pmod m),\\ &\vdots\\ \frac{m-1}{2} &\equiv \frac{m-1}{2} \pmod m), \end{aligned}$$

mientras que $-\dfrac{m-1}{2}+i-1 \equiv \dfrac{m-1}{2}+i \pmod m),\ \ i=1,2,...,\dfrac{m-1}{2}.$

- Si p es primo, existe $b \in \mathbb{Z}$ tal que $\mathbb{Z}_m = \{0,b,b^2,...,b^{p-1}\}$ (ver capítulo 5).

Ejemplo 3.12

$$\begin{aligned} \mathbb{Z}_5 &= \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\}\\ &= \{\overline{-2},\overline{-1},\overline{0},\overline{1},\overline{2}\} \quad \text{pues} \quad -2 \equiv 3 \pmod 5) \quad \text{y} \quad -1 \equiv 4 \pmod 5),\\ &= \{\overline{0},\overline{3},\overline{3^2},\overline{3^3},\overline{3^4}\} \quad \text{pues} \quad 3^2 \equiv 4 \pmod 5),\ 3^3 \equiv 2 \pmod 5),\ 3^4 \equiv 1 \pmod 5) \end{aligned}$$

Suma y producto en $\mathbb{Z}_m$. Ahora nos interesa ver $\mathbb{Z}_m$ desde el punto de vista de su estructura algebraica. Esto no solo nos permite usar un lenguaje común, sino que también nos permite usar resultados generales de la teoría de grupos, por ejemplo.

Podemos definir operaciones de suma y producto en $\mathbb{Z}_m$ de la siguiente manera:

$\overline{a}+\overline{b} = \overline{\text{rem}(a+b,m)}$ i.e. $\overline{a}+\overline{b}$ es el resto de dividir $a+b$ por m

$\overline{a}\cdot\overline{b} = \overline{\text{rem}(a\cdot b,m)}$ i.e. $\overline{a}\cdot\overline{b}$ es el resto de dividir $a\cdot b$ por m

Ejemplo 3.13

En $\mathbb{Z}_7$,

$$\overline{5}+\overline{6}=\overline{\text{rem}\,117}=\overline{4}$$

$$\overline{5}\cdot\overline{30}=\overline{\text{rem}(150,7)}=\overline{3}$$

Propiedades de la suma y producto en $\mathbb{Z}_m$. Con estas operaciones, si $m\geq 2$, $\mathbb{Z}_m$ es *anillo conmutativo* con identidad. Si $\overline{a},\overline{b},\overline{c}\in\mathbb{Z}_m$,

(1) $\overline{a}+\overline{b}\in\mathbb{Z}$,

(2) $\overline{a}+\overline{b}=\overline{b}+\overline{a}$,

(3) $\overline{a}+(\overline{b}+\overline{c})=(\overline{a}+\overline{b})+\overline{c}$,

(4) $\overline{a}+\overline{0}=\overline{0}+\overline{a}=\overline{a}$,

(5) el inverso aditivo de $\overline{a}$ es $\overline{-a}$

(1′) $\overline{a}\cdot\overline{b}\in\mathbb{Z}$,

(2′) $\overline{a}\cdot(\overline{b}+\overline{c})=\overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$ y $(\overline{b}+\overline{c})\cdot\overline{a}=\overline{b}\cdot\overline{a}+\overline{c}\cdot\overline{a}$,

(3′) $\overline{a}\cdot\overline{1}=\overline{a}$.

Inversos módulo m (unidades) y divisores de cero. Sea $a\in\mathbb{Z}_m$, a *es una unidad si tiene inverso, es decir, si existe $b\in\mathbb{Z}_m$ tal que $ba\equiv ab\equiv 1 \pmod m$.* En este caso ponemos $a^{-1}=b$. Por ejemplo, $2\cdot 3\equiv 1 \pmod 5$, entonces el inverso de 2, módulo 5, es 3 y viceversa.

Por otra parte, $\overline{a}\neq\overline{0}$, es divisor de cero en $\mathbb{Z}_m$ si existe $\overline{b}\in\mathbb{Z}_m$, $\overline{b}\neq\overline{0}$, tal que $\overline{ab}=\overline{0}$. Por ejemplo, $2\cdot 3\equiv 0 \pmod 6$, entonces 2 y 3 son divisores de cero en $\mathbb{Z}_6$.

Teorema 3.4

En $\mathbb{Z}_m$,

a.) $\overline{a}$ es una unidad si y solo si $\text{mcd}\,(a,m)=1$;

b.) $\overline{a}$ es divisor de cero si y solo si $1<\text{mcd}\,(a,m)<m$;

Prueba: **a.)** $ab\equiv 1 \pmod m$ si y solo si existe $k\in\mathbb{Z}$ tal que $ab+mk=1$, es decir, si y solo si $\text{mcd}\,(a,m)=1$.

b.) Sea $a>1$ y $d=\text{mcd}\,(a,m)$.
" $\Longrightarrow$ " Como a es divisor de cero, sea $\overline{b}\neq\overline{0}$, tal que $\overline{ab}=\overline{0}$. Supongamos, por contradicción, que $d=1$ o $d=m$. Si $d=1\,\wedge\, m|ab \implies m|b$, pero esto no puede ser pues $b\not\equiv 0(\text{mod}\,m)$. Si $d=m \implies m|a$ pero esto no puede ser pues $a\not\equiv 0(\text{mod}\,m)$.

" $\Longleftarrow$ " Como $1<d<m$ y $d|m$, existe k tal que $dk=m$ y $1<k<m$. Entonces $\overline{k}\neq\overline{0}$ y $\overline{dk}=\overline{0}$. Por tanto, si $a=dk'$, $\overline{ak}=\overline{dkk'}=\overline{0}$, es decir, a es divisor de cero.

Inversos y módulo primo. Si p es primo, entonces $\text{mcd}\,(i,p)=1$ para todo $i=1,2,...,p-1$. Así, en $\mathbb{Z}_p$ todo elemento tiene inverso y no hay divisores de cero. $\mathbb{Z}_m$ es un *campo* si y solo si

Ejemplo 3.14 (Unidades y divisores de cero).

Sea $m = 9$. Si construimos una tabla de multiplicar para $\mathbb{Z}_9$ podemos detectar las unidades y los divisores de cero (si hubiera). La otra manera es usar el teorema (3.4)

$(\mathbb{Z}_9, \cdot)$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8

Tabla 3.2. Tabla de multiplicar para $\mathbb{Z}_9$

a	1	2	3	4	5	6	7	8
mcd $(a,9)$	1	1	3	1	1	3	1	1

Tabla 3.3. Aplicando el teorema (3.4)

Así, las unidades de $\mathbb{Z}_8$ son $1,2,4,5,7,8$ y los divisores de cero son $3,6$.

m es primo.

En el mundillo del álgebra, si p es primo, se usa a $\mathbb{Z}_p$ como el "representante" de los campos finitos con p elementos y se le denota $\mathbb{F}_p$.

Sistemas de residuos. Como ya dijimos, hay distintos conjuntos de representantes de $\mathbb{Z}_m$. Vamos a establecer un par de lemas que serán de mucha utilidad la hora de establecer los teoremas clásicos en teoría de números.

¿Cómo determinar si dado $\{a_1, a_2, ..., a_m\}$, se tiene $\mathbb{Z}_m = \{a_1, a_2, ..., a_m\}$?.

$\mathbb{Z}_m = \{a_1, a_2, ..., a_m\}$ si todos los m $a_i's$ están en clases distintas, es decir,

$$\{\overline{a_1},\, \overline{a_2},\, \ldots,\, \overline{a_m}\} = \{\,\overline{\text{rem}(a_1, m)},\; \overline{\text{rem}(a_2, m)}, \ldots,\; \overline{\text{rem}(a_m, m)}\} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\},$$

Para comprobaciones en la teoría usaríamos la siguiente caracterización: $\mathbb{Z}_m = \{a_1, a_2, ..., a_m\}$ si y sólo si $a_i \not\equiv a_j \pmod m$ $\forall i, j$ con $i \neq j$, $1 \leq i, j \leq m$.

Lema 3.1

Sea $\text{mcd}\,(a, m) = 1$, entonces $\mathbb{Z}_m = \{0,\, a,\, a \cdot 2, \ldots, a \cdot (m-1)\}$

Prueba: Solo hay que probar que los m elementos de $\{0,\, a,\, a \cdot 2, \ldots, a \cdot (m-1)\}$ no se repiten módulo m.

Primero observemos que si $i, j \in \{0, 1, 2, ..., m-1\}$ y si $i \neq j$, entonces $j \not\equiv i \pmod m$ pues i y j estarían en clases distintas.

Ahora, si $a \cdot i \equiv a \cdot j \pmod m$ con $i \neq j$, $1 \leq i, j \leq m$, entonces $m | a(j-i)$; pero $\text{mcd}\,(a, m) = 1$ entonces $m | (j-i)$ pero esto es imposible pues $j \not\equiv i \pmod m$.

La aplicación práctica que vamos a encontrar frecuentemente es la que se establece en el siguiente corolario,

Corolario 3.1 *Si* $\operatorname{mcd}(a,m)=1$, *entonces*

$$a\cdot 1\ \cdot\ a\cdot 2\cdots a\cdot(m-1)\equiv 1\cdot 2\ \cdots\ (m-1)\ (\operatorname{mod} m)$$

Prueba: Ejercicio.

Ejemplo 3.15

$\operatorname{mcd}(4,5)=1$, entonces $4\cdot 1\ \cdot\ 4\cdot 2\cdot 4\cdot 3\ \cdot\ 4\cdot 4\equiv 1\cdot 2\cdot 3\cdot 4\ (\operatorname{mod} 5)$ o $6144\equiv 24\ (\operatorname{mod} 5)$.

3.6 Congruencias lineales

Es fácil resolver la ecuación $x+a\equiv b\ (\operatorname{mod} m)$, la solulción es $x\equiv b-a\ (\operatorname{mod} m.)$

Consideremos la ecuación $ax\equiv b\ (\operatorname{mod} m)$: Hay un $k\in\mathbb{Z}$ tal que $b-ax=mk$ o $b=mk+ax$. Como ya vimos en la sección sobre ecuaciones diofánticas lineales, $b=mk+ax$ tiene solución si y sólo si $\operatorname{mcd}(a,m)|b$. Si esta es la situación, hay un $k'\in\mathbb{Z}$ tal que $b=k'\cdot\operatorname{mcd}(a,m)$ y entonces, utilizando el algoritmo extendido de Euclides, determinamos $s,t\in\mathbb{Z}$ tal que $\operatorname{mcd}(a,b)=sa+tm \implies b=k'sa+k'tm$ y una solución sería $x=k's$.

Ejemplo 3.16

Determinar una solución de $2x\equiv 5\ (\operatorname{mod} 7)$.

Solución: Como $\operatorname{mcd}(2,7)=1$ y $1|5$, la ecuación tiene solución. Como el módulo es pequeño, podemos encontrar una solución por *ensayo y error*: Sustituimos los valores $x=0,1,2,...,6$ y buscamos los valores de x que satisfacen la congruencia. En este caso obtenemos la solución $x=6$. Esta solución es única módulo 7.

Si el módulo es muy grande, podemos encontrar una solución usando algoritmo extendido de Euclides: $1=-3\cdot 2\ +\ 1\cdot 7 \implies 5=-15\cdot 2\ +\ 5\cdot 7$. Así, $x=-15$ es una solución. La reducción módulo 7 nos da $x=6$.

Inversos módulo m

Teorema 3.5

Si $\operatorname{mcd}(a,m)=1$ entonces $ax\equiv 1\ (\operatorname{mod} m)$ tiene solución única $x=a^{-1}$ módulo m.

Prueba: Resolver la congruencia $ax\equiv 1\ (\operatorname{mod} m)$ es equivalente a resolver la ecuación $ax+my=1$. Como $\operatorname{mcd}(a,m)=1$, existen $s,t\in\mathbb{Z}$ tal que $sa+tm=1$, con lo que tenemos la solución

$x = s$ para la ecuación $ax \equiv 1 \pmod{m}$.
La unicidad módulo m significa que si $as \equiv 1 \pmod{m}$ y $as' \equiv 1 \pmod{m}$, entonces $s \equiv s' \pmod{m}$. Para verificar que la solución es única módulo m, supongamos que $as' \equiv 1 \pmod{m}$, luego, restando tenemos $a(s-s') \equiv 0 \pmod{m} \implies m|a(s-s')$ pero como $\text{mcd}(a,m) = 1$ entonces $m|(s-s') \implies s \equiv s' \pmod{m}$.

Si $sa + tm = 1$, en la práctica tomamos $a^{-1} = \text{rem}(s,m)$ (el residuo de dividir s por m en el teorema de la división).

Ejemplo 3.17

Como $\text{mcd}(27,31) = 1$ entonces 27 tiene inverso módulo 31. Aplicando el algoritmo extendido de Euclides obtenemos $-8 \cdot 27 + 7 \cdot 31 = 1$. Así $a^{-1} = -8$. En la práctica nos interesa la solución $a^{-1} = \text{rem}(-8,31) = 23$ (pues $-8 = -1 \cdot 31 + 23$).

Solución general. Podemos aplicar la teoría de ecuaciones diofánticas lineales para obtener el siguiente resultado,

Teorema 3.6

$ax \equiv b \pmod{m}$ tiene solución si y sólo si $d = \text{mcd}(a,m)|b$. Si x_0 es una solución particular, la solución general es $x \equiv x_0 \pmod{m/d}$, es decir, obtenemos las 'd' soluciones módulo m, $x = x_0 + \frac{m}{d}t$ con $0 \leq t < d$

Prueba: Para la prueba vamos a usar los teoremas (2.11) y (2.13) de la sección de ecuaciones diofánticas. Si $ax \equiv b \pmod{m}$, entonces hay un $k \in \mathbb{Z}$ tal que $ax - mk = b$. Esta ecuación diofántica tiene solución si y solo si $d = \text{mcd}(a,m)|b$. Si una solución particular es $x = x_0$, entonces la solución general es $x = x_0 + \frac{m}{d}t$, con $t \in \mathbb{Z}$ (aquí solo interesa x). Solo falta probar que solo hay d soluciones distintas módulo m.
Si $x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod{m}$, usando el hecho de que $(m/d)|m$, obtenemos que $t_1 \equiv t_2 \pmod{d}$, es decir, $x_0 + \frac{m}{d}t_1$ y $x_0 + \frac{m}{d}t_2$ son soluciones distintas módulo m si y solo si t_1 y t_2 están en clases distintas de $\mathbb{Z}_d$. Esto nos deja solo las d posibilidades $t = 0,1,...,d-1$.

Corolario 3.2 *Si p es primo y $\text{mcd}(a,p) = 1$, la ecuación lineal $ax \equiv b \pmod{m}$ tiene solución única $x \equiv a^{-1}b \pmod{p}$.*

Prueba: Ejercicio.

Ejemplo 3.18

a.) Resolver $2x \equiv 5 \pmod 7$.

Solución: como $\text{mcd}(2,7) = 1$, la ecuación tiene solución única módulo 7. La solución es $x \equiv 2^{-1} \cdot 5 \pmod 7$; como $4 \cdot 2 \equiv 1 \pmod 7$, $x \equiv 4 \cdot 5 \equiv 6 \pmod 7$. Así, la solución es $x = 6$.

b.) Resolver $42x \equiv 50 \pmod{76}$.

Solución: Usando el algoritmo extendido de Euclides obtenemos la solución particular

$$x = -225 \equiv 3 \pmod{76}.$$

Ahora, como $\text{mcd}(42,76) = 2$, la solución general es

$$x \equiv 3 \pmod{38},$$

es decir, $x = 3 + 38t$. La ecuación tiene dos soluciones módulo 76, a saber $x = 3$ y $x = 41$.

c.) Resolver $12x \equiv 48 \pmod{18}$.

Solución: Una solución particular es $x = 1$, ahora, como $\text{mcd}(12,18) = 6$, la solución general es $x \equiv 1 \pmod 3$, es decir, $x = 1 + 3t$. La ecuación tiene seis soluciones módulo 18, a saber $x = 1, 4, 7, 10, 13$ y 16.

d.) La ecuación $2x \equiv 3 \pmod 4$ no tiene solución pues $\text{mcd}(2,4) = 2 \nmid 3$

3.7 Teorema Chino del resto

Un ejemplo concreto de un sistema de congruencias lineales se describe en el ejemplo que sigue,

Ejemplo 3.19

Calcule x tal que $\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 2 \pmod 5, \\ x \equiv 3 \pmod 7. \end{cases}$

Solución: Hay un número infinito de soluciones para este sistema, por ejemplo $x = 52, -53, 157, \ldots$ como se puede verificar rápidamente. Una manera de resolver este sistema es despejar y sustituir x hasta que la última congruencia sea usada,

$$
\begin{aligned}
x \equiv 1 \pmod 3 \quad &\Longrightarrow \quad x = 1 + 3t_1 \\
&\Longrightarrow \quad 1 + 3t_1 \equiv 2 \pmod 5 \\
&\Longrightarrow \quad 3t_1 \equiv 1 \pmod 5 \\
&\Longrightarrow \quad t_1 \equiv 2 \pmod 5 \quad \text{pues} \quad 3 \cdot 2 \equiv 1 \pmod 5 \\
&\Longrightarrow \quad t_1 = 2 + 5t_2 \\
&\Longrightarrow \quad x = 7 + 15t_2 \\
&\Longrightarrow \quad 7 + 15t_2 \equiv 3 \pmod 7 \\
&\Longrightarrow \quad 15t_2 \equiv 3 \pmod 7 \\
&\Longrightarrow \quad t_2 \equiv 3 \pmod 7 \quad \text{pues} \quad 15 \cdot 1 \equiv 1 \pmod 7
\end{aligned}
$$

$$
\begin{aligned}
\text{Por tanto,} \quad & t_2 = 3 + 7t \\
\text{y} \quad & x = 7 + 15 \cdot (3 + 7t) = 52 + 105t, \; t \in \mathbb{Z}.
\end{aligned}
$$

Así, $x = 52 + 105t$, $t \in \mathbb{Z}$; es la solución general del sistema. Aquí debemos notar que $105 = 3 \cdot 5 \cdot 7$, es decir, la solución es única módulo $3 \cdot 5 \cdot 7$.

Teorema 3.7 (Teorema Chino del resto).

Consideremos el sistema lineal de congruencias

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_k \pmod{m_k}
\end{aligned}
$$

con $\operatorname{mcd}(m_i, m_j) = 1$, $i \neq j$; entonces, si $M = m_1 \cdot m_2 \cdots m_k$, $M_i = M/m_i$ y $y_i \equiv M_i^{-1} \pmod{m_i}$, el sistema tiene solución única $x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_kM_ky_k$, módulo M.

Prueba: La prueba[3] es en dos partes, primero se muestra una solución de manera explícita y luego se prueba que es única.

Sean $M = m_1 \cdot m_2 \cdots m_k$ y $M_i = M/m_i$, $1 \leq i \leq k$. Como los módulos son primos relativos dos a dos, $\text{mcd}\,(M_i, m_i) = 1$ para cada i. También, $M_i \equiv 0 \pmod{m_j}$ $j \neq i$.

Como $\text{mcd}\,(M_i, m_i) = 1$, entonces $M_i y_i \equiv 1 \pmod{m_i}$ tiene solución única $y_i \equiv M_i^{-1} \pmod{m_i}$.

Sea $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_k M_k y_k$. Vamos a mostrar que x es solución del sistema de congruencias.

$$\begin{aligned} x &= \sum_{\substack{i=1 \\ i\neq j}}^{k} a_i M_i y_i \;+\; a_j M_j y_j \\ &\equiv \sum_{\substack{i=1 \\ i\neq j}}^{k} a_i \cdot 0 \cdot y_i \;+\; a_j \cdot 1 \pmod{m_j} \\ &\equiv 0 + a_j \pmod{m_j} \\ &\equiv a_j \pmod{m_j},\;\; 1 \leq j \leq k \end{aligned}$$

Por tanto, x satisface todas las congruencias del sistema, es decir, es una solución del sistema.

Para probar la unicidad módulo M supongamos que x_1 y x_2 son soluciones del sistema, vamos a demostrar que $x_1 \equiv x_2 \pmod{M}$.

Puesto que $x_1 \equiv a_j \pmod{m_j}$ y $x_2 \equiv a_j \pmod{m_j}$ para $1 \leq j \leq k$, restando $x_1 - x_2 \equiv 0 \pmod{m_j}$, luego $m_j | (x_1 - x_2)$ para cada j.

Entonces $\text{mcm}\,(m_1 \cdot m_2 \cdots m_k) | (x_1 - x_2)$, es decir, $M | (x_1 - x_2)$ pues también $M = \text{mcm}\,(m_1 \cdot m_2 \cdots m_k)$. Por tanto, $x_1 - x_2 \equiv 0 \pmod{M}$, es decir $x_1 \equiv x_2 \pmod{M}$.

Ejemplo 3.20

Resolver el sistema $\begin{cases} x \equiv 1 \pmod{3}, \\ x \equiv 2 \pmod{5}, \\ x \equiv 3 \pmod{7}. \end{cases}$ usando el método del teorema anterior.

Solución: $M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = 35$, $M_2 = 21$, $M_3 = 15$. Luego,

[3] Para seguir la prueba debemos recordar que si $m_1, m_2, ..., m_k$ son primos relativos dos a dos, entonces $\text{mcm}\,(m_1, m_2, ..., m_k) = m_1 \cdot m_2 \cdots m_k$ y si $m_1, m_2, ..., m_k$, $a \in \mathbb{Z}^+$ y $m_i | a$, $i = 1, 2, ..., k$; entonces $\text{mcm}\,(m_1, m_2, ..., m_k) | a$.

$y_1 \equiv M_1^{-1} \pmod 3 \implies y_1 \equiv 2 \pmod 3$
$y_2 \equiv M_2^{-1} \pmod 5 \implies y_2 \equiv 1 \pmod 5$
$y_3 \equiv M_3^{-1} \pmod 7 \implies y_3 \equiv 1 \pmod 7$

Así,

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \\ &= 157 \equiv 52 \pmod M \end{aligned}$$

Podemos decir, la solución única es $x \equiv 52 \pmod{105}$.

Sistemas con módulos no coprimos dos a dos. Si los módulo no son coprimos dos a dos, el sistema podría tener solución en las condiciones del siguiente teorema,

Teorema 3.8

El sistema

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

tiene solución si y solo si $\operatorname{mcd}(m_i, m_j) | (a_i - a_j)$, $1 \leq i, j \leq k$. Cuando hay solución, es única módulo $\operatorname{mcm}(m_1 \cdot m_2 \cdots m_k)$.

Si hay solución, se puede obtener despejando y sustituyendo como en el ejemplo (3.19).

3.8 Congruencias de Orden Superior

Consideremos de manera general el problema de resolver la congruencia $P(x) \equiv 0 \pmod m$ con $P(x)$ un polinomio con coeficientes enteros. La manera directa (y no muy eficiente) de resolver este problema es probar con $x = 0, 1, ..., m-1$.

Ejemplo 3.21

Resolver $x^2 + x - 2 \equiv 0 \pmod{10}$.

Solución: Probamos sustituyendo $x = 0, 1, ..., 9$ y encontramos las soluciones $x = 1, 3, 6, 8$.

Si m no es la potencia de un primo, el problema se puede reducir a resolver un sistema con módulos menores que m, usando el teorema chino del resto.

Teorema 3.9

Sea $m = m_1 \cdot m_2 \cdots m_k$ con $m_1, m_2, \cdots, m_k$ primos relativos dos a dos. $x = a$ es una solución de $P(x) \equiv 0 \pmod{m}$ si y solo si a es solución del sistema

$$\begin{array}{c} P(x) \equiv 0 \pmod{m_1} \\ P(x) \equiv 0 \pmod{m_2} \\ \ldots \\ P(x) \equiv 0 \pmod{m_k} \end{array}$$

Prueba: Si $P(a) \equiv 0 \pmod{M}$, entonces $P(a) \equiv 0 \pmod{m_i}$, $i = 1, 2, ..., k$.
Ahora supongamos que $x = a$ es solución del sistema, es decir,

$$\begin{array}{c} P(a) \equiv 0 \pmod{m_1} \\ P(a) \equiv 0 \pmod{m_2} \\ \ldots \\ P(a) \equiv 0 \pmod{m_k} \end{array}$$

El teorema chino del resto nos dice que $P(a) \equiv 0 \pmod{m_1 \cdot m_2 \cdots m_k}$, es decir, $x = a$ es solución de $P(x) \equiv 0 \pmod{m}$.

Ejemplo 3.22

Resolver $x^2 + x - 2 \equiv 0 \pmod{10}$.

Solución: Como $10 = 2 \cdot 5$, podemos resolver el sistema

$$\begin{array}{c} P(x) \equiv 0 \pmod{2} \\ P(x) \equiv 0 \pmod{5} \end{array}$$

La ganancia sería resolver congruencias con un módulo más pequeño. Por ensayo y error,

$$\begin{array}{l} P(x) \equiv 0 \pmod{2} \text{ tiene soluciones } x = 0,1 \\ P(x) \equiv 0 \pmod{5} \text{ tiene soluciones } x = 1,3 \end{array}$$

La solución del problema requiere resolver los cuatro sistemas

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{5} \end{cases}, \begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 3 \pmod{5} \end{cases}, \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{5} \end{cases}, \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 3 \pmod{5} \end{cases}.$$

Las solución de cada uno de los cuatro sistemas son $x = 6, 8, 1, 3$, respectivamente. Por tanto, la solución de la congruencia $x^2 + x - 2 \equiv 0 \pmod{10}$ es $x = 1, 3, 6, 8$.

EJERCICIOS

3.1 Sea r el residuo de dividir b por m en el Teorema de la División. Dé un contra-ejemplo que evidencie que "$b \equiv r \pmod{m} \not\Longrightarrow b = r \bmod m$".¿Cuál es el requisito para la equivalencia?

3.2 Calcule el inverso de $a = 7$ módulo $m = 211$.

3.3 Si llamamos a los días de la semana por un número $0 \leq d < 7$ ($0 =$ domingo, $6 =$ sábado), describa un algoritmo (usando congruencias) que, sabiendo que hoy es el día d, nos diga qué día será en n días contando el día de hoy? Por ejemplo, si hoy es domingo (0), en 7 días es domingo. Por ejemplo, si hoy es lunes($d = 1$), ¿qué día es en 374 días?.

3.4 Probar que todo entero es congruente con exactamente uno de los residuos $\{0,1,2,...,m-1\}$ módulo m.

3.5 Muestre que todo primo $p > 3$ es congruente con 1 o con 5 módulo 6. **Ayuda:** Use el ejercicio anterior.

3.6 Sea $S = \{2,3,5,7,11,13,17,...\} = \{2,3\} \cup \{6k \pm 1 : k = 1,2,...\}$. Muestre que S contiene a todos los primos.
Ayuda: $2,3 \in S$. Solo falta verificar que si p es primo > 3, entonces $p \in S$.

3.7 Muestre que si p es primo y $p \nmid a$, la ecuación $ax \equiv b \pmod{p}$ tiene solución única, módulo p, $x \equiv a^{p-2}b \pmod{p}$.

3.8 ¿$\mathbb{Z}_7 = \{0,1,-2,4,-8,16,-32\}$?

3.9 Mostrar que si $a \in Z$, $Z_m = \{a, a+1, \ldots, a+m-1\}$.

3.10 Mostrar que si m es impar, $\mathbb{Z}_m = \{-\dfrac{m-1}{2}, \ldots, -1, 0, 1, \ldots \dfrac{m-1}{2}\}$

3.11 Muestre que si $\operatorname{mcd}(b,m) > 1$, entonces $\mathbb{Z}_m \neq \{0, b\cdot 1, b\cdot 2, \ldots, b\cdot(m-1)\}$

3.12 Sea p primo, muestre que si $\operatorname{mcd}(a,p) = 1$, entonces $\operatorname{mcd}(a^{-1},p) = 1$.

3.13 Muestre que si $k \geq 5$ entonces $k! \equiv 0 \pmod{15}$

3.14 Muestre que $3! + 4! + 5! + \cdots + 100!$ es divisible por 15.

3.15 Muestre que $N = 11 \cdot 14^n + 1$ es compuesto.
Ayuda: Si n es par, iniciar con $14 \equiv -1 \pmod{3}$ y recalcular N módulo 3. Si n es impar, iniciar con $14 \equiv -1 \pmod{5}$ y recalcular N módulo 5.

3.16 Muestre que si $P(x)$ es un polinomio con coeficientes enteros y si $a \equiv b \pmod{m}$ entonces $P(a) \equiv P(b) \pmod{m}$.

3.17 Dé un ejemplo que muestre que $(a \equiv b \pmod{p}$ y si $p|m) \not\Longrightarrow a \equiv b \mod (m)$

3.18 Sea p un divisor no trivial de m. Muestre que si $x_i \equiv x_j \pmod{p} \wedge x_i \not\equiv x_j \mod (m)$, entonces $\operatorname{mcd}(x_i - x_j, m)$ es un divisor no trivial de m.

3.19 Muestre que si $p \equiv 1 \pmod{4}$ y $p \equiv 1 \pmod{3}$, entonces $p \equiv 1 \pmod{12}$. **Ayuda:** Corolario (2.7).

3.20 Muestre que si $p \equiv 3 \pmod{4}$ y $p \equiv 2 \pmod{3}$, entonces $p \equiv 7 \pmod{12}$. **Ayuda:** Corolario (2.7).

3.21 Muestre que $4^{3q} \equiv 1 \pmod{9}$, $q \in \mathbb{N}$.

3.22 Muestre que para cada $n \in \mathbb{N}$, $4^n \equiv 1 \pmod{9}$ o $4^n \equiv 4 \pmod{9}$ o $4^n \equiv 7 \pmod{9}$
Ayuda: Calcule primero $4^t \bmod 9$ para $t = 0,1,2,3$. Luego use el algoritmo de la división: $4^n = 4^{3q+r}$.

3.23 Muestre que $6 \cdot 4^n \equiv 6 \pmod{9}$ para todo $n \geq 0$.

3.24 Muestre que $(a_1 + a_2)^2 \equiv (a_1^2 + a_2^2) \pmod{2}$

3.25 Muestre que $(a_1 + a_2 + ... + a_n)^2 \equiv (a_1^2 + a_2^2 + ... + a_n^2) \pmod{2}$

3.26 Muestre que si $0 \leq r < m$ y $a \equiv r \pmod{m}$, entonces $a \bmod m = r$

3.27 Sean $m_1, m_2, ..., m_k \in \mathbb{Z}^+$ con $c = \text{mcm}(m_1 m_2 \cdots m_k)$. Muestre que si $a \equiv b \pmod{m_i}$, $i = 1, 2, ..., k$; entonces $a \equiv b \pmod{c}$.

3.28 Verifique que $11^2 \equiv 1 \pmod{5}$ y $11 \equiv 1 \pmod{5}$ pero $11 \not\equiv -1 \mod 5$

3.29 Muestre que si p es primo y si $\text{mcd}(a, p) = 1$, entonces si $a^2 \equiv 1 \pmod{p} \implies a \equiv 1 \pmod{p}$ o $a \equiv -1 \pmod{p}$. Indique además, ¿porqué se requiere la hipótesis $\text{mcd}(a, p) = 1$,?

3.30 Sea p primo impar y $i, j \in \{-\frac{p-1}{2}, \ldots, -1, 0\, 1, \ldots \frac{p-1}{2}\}$ con $i \neq j$. Muestre que $i^2 \not\equiv j^2 ($ mod $p)$

3.31 Sea p primo y $i, j \in \{0, 1, 2, ..., p-1\}$ con $i \neq j$. Muestre que $i^2 \not\equiv j^2 (\mod p)$

3.32 Muestre que $a^2 \equiv a \pmod{2}$ para todo $a \in \mathbb{Z}$

3.33 Muestre que si $ra \equiv rb \pmod{rm}$ entonces $a \equiv b \pmod{m}$.

3.34 Sean a, b enteros positivos $< m$. Muestre que $a \not\equiv b(\mod m)$

3.35 Dé un ejemplo en el que $\text{mcd}(a, m) = 1$ y $\text{mcd}(b, m) = 1$ y que $a \equiv b \pmod{m}$.

3.36 Calcule el más pequeño entero positivo n que deja residuo 3 al dividir por 7, residuo 4 al dividir por 9 y residuo 8 cuando se divide por 11.

3.37 Resuelva el sistema

$$\begin{aligned} x &\equiv 21 \pmod{3}, \\ x &\equiv 32 \pmod{5}, \\ x &\equiv 3 \pmod{7}, \\ x &\equiv 9 \pmod{11}, \\ x &\equiv 2 \pmod{2}, \\ x &\equiv 1 \pmod{97}. \end{aligned}$$

3.38 Un niño tiene una bolsa con bolinchas. Si las agrupa en puños de 7, le sobran 5, Si las agrupa en puños de 11, le sobran 6, Si las agrupa en puños de 13, le sobran 8. Determine el mínimo número de bolinchas que podría tener el niño.

3.39 Muestre que el sistema $\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{6} \end{cases}$ no tiene solución. **Ayuda:** Use el método de sustitución y Bezout.

3.40 Calcule el más pequeño entero positivo n tal que $2|n$, $3|n+1$, $5|n+2$, $7|n+3$, y $11|n+4$.

3.41 Resuelva el sistema

$$\begin{aligned} x &\equiv 4 \pmod{6}, \\ x &\equiv 2 \pmod{8}, \\ x &\equiv 1 \pmod{9}. \end{aligned}$$

3.42 Resolver $x^5 - 3x^4 + x - 2 \equiv 0 \pmod{165}$.



4 POTENCIAS mod m

4.1 Orden de un elemento módulo m.

Sea $\text{mcd}(a,p)=1$, entonces $p \nmid a^s$ si $s \geq 1$. Como $a,a^2,a^3,...,a^p$ son p elementos no nulos del conjunto de $p-1$ residuos $\{1,2,...,p-1\}$, entonces al menos dos se tienen que repetir módulo p: Existen $s \neq t$ tal que $a^s \equiv a^t \pmod{p}$.

La parte importante aquí es ver que si $s=t+r$, entonces, como $\text{mcd}(a^t,p)=1$, a^t tiene inverso módulo p, así multiplicando este inverso a ambos lados se tienen

$$a^s \equiv a^t \pmod{p} \implies a^{t+r} \equiv a^t \pmod{p} \implies a^r \equiv 1 \pmod{p}.$$

Ejemplo 4.1

En $\mathbb{Z}_7$, $\{2,2^2,2^3,2^4,2^5,2^6,2^7\}=\{2,4,1,2,4,1,2\}$. En particular, $2^2 \equiv 2^5 \pmod{7}$, entonces $2^3 \equiv 1 \pmod{7}$

Teorema 4.1

Si $\text{mcd}(a,m)=1$ entonces $a^t \equiv 1 \pmod{m}$ para algún $1 \leq t < m$.

Prueba: Se trata de refinar un poco el argumento que se dio más arriba, así que se deja como ejercicio.

Definición 4.1 (Orden de un número módulo m).

Sea $m \geq 2$. Si $\text{mcd}(a,m)=1$, el orden de "a" módulo m, denotado $\text{Ord}_m(a)$, es el más pequeño entero positivo t tal que $a^t \equiv 1 \pmod{m}$

Observe que si $\text{Ord}_m(a)=t$, entonces $a^t \equiv 1 \pmod{m}$ pero $a^s \not\equiv 1 (\text{mod}\, m)$ si $0 < s < t$

Ejemplo 4.2

El orden de 2 módulo 7 es $t=3$ pues $2^3 \equiv 1 \pmod 7$ pero $2^2 \not\equiv 1 (\bmod 7)$ y $2^1 \not\equiv 1 (\bmod 7)$. Observemos que $2^6 \equiv 1 \pmod 7$ y $3|6$.

Teorema 4.2

Si $\text{Ord}_m(a) = t$ y $a^s \equiv 1 \pmod m$, entonces $t|s$.

Prueba: Si $s = kt + r$ con $0 \leq r < t$, se tiene que $a^s \equiv a^{kt+r} \pmod m \implies a^r \equiv 1 \pmod m$. Pero como $0 \leq r < t$ y t es el orden de a, la única posibilidad que queda es $a^r \equiv 1 \pmod m$ solo si $r = 0$.

Si conocemos el orden de un número módulo m, podríamos ganar algo en el cálculo del orden de otros elementos de $\mathbb{Z}_m$: Si a tiene orden t módulo m y queremos calcular el orden de a^d, ya se sabe que $a^{dt} \equiv 1 \pmod m$ pero el orden de a^d es $\leq dt$, en realidad tenemos,

Teorema 4.3

Si $\text{Ord}_m(a) = t$, entonces el orden de a^d es $q = \dfrac{t}{\text{mcd}\,(d,t)}$ si $d > 0$

Prueba: $a^{\text{mcm}(d,t)} \equiv 1 \pmod m$ pues $t|\,\text{mcm}\,(d,t)$. Tenemos,

$$(a^d)^{\frac{\text{mcm}(d,t)}{d}} \equiv 1 \pmod m$$

Como $\text{mcm}\,(d,t) = \dfrac{dt}{\text{mcd}\,(d,t)} \implies \dfrac{\text{mcm}\,(d,t)}{d} = \dfrac{t}{\text{mcd}\,(d,t)}$, entonces

$$(a^d)^{\frac{t}{\text{mcd}(d,t)}} \equiv 1 \pmod m$$

Falta probar que el orden de a^d es $\dfrac{t}{\text{mcd}\,(d,t)}$: Si $(a^d)^s = a^{ds} \equiv 1 \pmod m$ entonces $t|ds$. Así, ds es múltiplo de t y es múltiplo de d, por tanto,

$$ds \geq \text{mcm}\,(d,t) \implies s \geq \frac{\text{mcm}(d,t)}{d} = \frac{t}{\text{mcd}\,(d,t)}.$$

Ejemplo 4.3

El orden de 2 módulo 7 es $t = 3$, entonces el orden de $4 = 2^2$ es $\dfrac{3}{\text{mcd}\,(2,3)} = 3$, i.e. $4^3 \equiv 1 \pmod{7}.$

El orden de 3 módulo 163 es 162, entonces el orden de 3^{26} es $\dfrac{162}{\text{mcd}\,(26,162)} = 81.$

4.2 El Teorema "pequeño" de Fermat.

Para establecer el teorema "pequeño" de Fermat[4], observemos que

$$(a\cdot 1)\,(a\cdot 2)\cdots(a\cdot(p-1)) = a^{p-1}(1\cdot 2\cdots(p-1))$$

Pero podemos probar que si $\text{mcd}(a,p) = 1$, entonces el conjunto $\{a\cdot 1, a\cdot 2, \cdots, a\cdot(p-1)\}$ es una permutación módulo p, del conjunto $\{1,2,...,p-1\}$. Luego, si $\text{mcd}\,(a,p) = 1$, cancelando tendríamos $a^{p-1} \equiv 1 \pmod{p.}$

Ejemplo 4.4

Sea $a = 270$ y $p = 7$.

$270\cdot 1 \equiv 4 \pmod 7$ $\quad$ $270\cdot 2 \equiv 1 \pmod 7$
$270\cdot 3 \equiv 5 \pmod 7$ $\quad$ $270\cdot 4 \equiv 2 \pmod 7$
$270\cdot 5 \equiv 6 \pmod 7$ $\quad$ $270\cdot 6 \equiv 3 \pmod 7$

Así,

$$\begin{aligned} 270^6(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6) &\equiv (270\cdot 1)(270\cdot 2)(270\cdot 3)(270\cdot 4)(270\cdot 5)(270\cdot 6) \pmod 7 \\ &\equiv (4\cdot 5\cdot 6\cdot 1\cdot 2\cdot 3) \pmod 7 \end{aligned}$$

entonces, $270^6(1\cdot 2\cdots 6) \equiv (1\cdot 2\cdots 6) \pmod 7 \implies 270^6 \equiv 1 \pmod 7$

Antes de enunciar el teorema, establecemos el lema

[4] El 18 de octubre de 1640, Fermat escribió una carta a Bernhard Frenicle de Bessy (1605-1675), un funcionario de la Casa de la Moneda francesa, excelente alumno en teoría de los números.
En su carta, Fermat comunica el resultado siguiente: Si p es primo y $p \nmid a$ entonces $p | a^{p-1} - 1$. Fermat no presentó una prueba de este resultado, pero una nota adjunta prometía enviar una demostración, siempre que no resultara demasiado extensa. Sin embargo, la primera prueba conocida la dio Euler un siglo después. Este resultado es conocido como el "pequeño" teorema de Fermat para diferenciarlo del "último teorema de Fermat" (1637): La ecuación $x^n + y^n = z^n$ no tiene soluciones enteras positivas si $n > 2$ (demostrado por A.Wiles en 1995.)

P. Fermat (1601-1665)

Lema 4.1

Sea p primo y $\text{mcd}\,(a,p)=1$, entonces

$$a\cdot 1\ \cdot\ a\cdot 2\ \cdots\ a\cdot(p-1)\equiv 1\cdot 2\ \cdots\ (p-1)\pmod p$$

Prueba: Aplicación directa del lema (3.1) y el corolario (3.1)

Teorema 4.4 (Teorema "pequeño" de Fermat)

Sea p primo y $a\in\mathbb{Z}$.

- Si $\text{mcd}\,(a,p)=1$ entonces, $a^{p-1}\equiv 1\pmod p$
- Para cualquier $a\in\mathbb{Z}^+$ se tiene $a^p\equiv a$ (mod p.)

Prueba: Usando lema anterior,

$$\begin{aligned} a^{p-1}(1\cdot 2\cdots(p-1)) &\equiv (a\cdot 1)(a\cdot 2)\cdots(a\cdot(p-1))\pmod p\\ &\equiv 1\cdot 2\cdots(p-1)\pmod p \end{aligned}$$

Entonces $a^{p-1}(1\cdot 2\cdots(p-1))\equiv 1\cdot 2\cdots(p-1)\pmod p \implies a^{p-1}\equiv 1\pmod p$ pues se sabe que $\text{mcd}\,(1\cdot 2\cdots(p-1),p)=1$.

Para probar la segunda afirmación solo hay que observar que si $p|a$ entonces $a\equiv 0\pmod p$ por tanto $a^p\equiv a\pmod p$. Si a y p son primos realtivos se obtiene el resultado de manera inmediata.

Ejemplo 4.5

Calcule manualmente el resto de dividir 24^{1937} por 17.

Solución: Por el teorema de Fermat, como $\text{mcd}\,(24,17)=1$, $24^{16}\equiv 1\pmod{17}$. Luego, como $1937=16\cdot 121+1$, entonces

$24^{1937}=24^{16\cdot 121+1}=24^{16\cdot 121}24^1\equiv 24\pmod{17}$, es decir, $24^{1937}\equiv 7\pmod{17}$.

Ejemplo 4.6

La congruencia $x^6 + x^4 + x - 3 \equiv 0 \pmod 5$ tiene las mismas soluciones que la congruencia $x^2 + x - 3 \equiv 0 \pmod 5$ pues, por el teorema de Fermat, $x^4 \equiv 1 \pmod 5$ y $x^6 = x^4 \cdot x^2 \equiv x^2 \pmod 5$

Teorema 4.5

Sea p primo y a cualquier entero tal que $p \nmid a$. Entonces, $\overline{a^{p-2}}$ es el inverso de $\overline{a}$ módulo p.

Prueba: Por el teorema de Fermat, $a^{p-1} \equiv 1 \pmod p$, entonces $a \cdot a^{p-2} \equiv 1 \pmod p$, es decir, $\overline{a} \cdot \overline{a^{p-2}} = \overline{1}$.

Corolario 4.1 *Sea $p > 1$. Si existe $a \in \mathbb{Z}$ y $\operatorname{mcd}(a,p) = 1$, tal que $a^p \not\equiv a \pmod p$, entonces p es compuesto.*

Prueba: Ejercicio.

El teorema de Fermat no se puede usar, en principio como una prueba de primalidad pues solo nos da una condición necesaria pero no suficiente. En efecto, hay números compuestos que pasan la "prueba" del teorema de Fermat para alguna base a.

Ejemplo 4.7

a.) $341 = 11 \cdot 31$ es compuesto, $\operatorname{mcd}(341,2) = 1$ y $2^{340} \equiv 1 \pmod{341}$, es decir, 341 pasa la "prueba de Fermat" en base 2 pero no es primo.

b.) 4 no es primo pues $2^4 \not\equiv 2 \pmod 4$.

4.3 Teorema de Euler

El teorema de Euler es uno de los grandes hitos en la desarrollo de la teoría de números. Fue probado por Euler en 1760. Este teorema extiende el teorema "pequeño" de Fermat a un módulo arbitrario. Antes de enunciarlo y probarlo, necesitamos algunos detalles técnicos.

Definición 4.2

Para cada $n \geq 1$, denotamos con $\varphi(n)$ la cantidad de enteros positivos menores que n y coprimos con n. A φ se le llama función "phi" de Euler.

Euler parece que no usaba una notación funcional para esta función; él usó en algún momento la notación "πn". Gauss introdujo la notación "$\varphi(n)$" aunque también se usa "$\phi(n)$". Sylverter introdujo la notación "Totient(n)" que a veces aparece en la literatura actual.

Ejemplo 4.8

$\varphi(24) = 8$ pues $1,5,7,11,13,17,19$ y 23 son los coprimos con 24 inferiores a 24.

Recordemos que $a \in \mathbb{Z}_m$ tiene inverso si $\operatorname{mcd}(a,m) = 1$. Luego, $\varphi(m)$ calcula la cantidad de unidades en $\mathbb{Z}_m$. Así, si p es primo, entonces $\varphi(p) = p - 1$.

Ejemplo 4.9

Sea $m = 9$, de acuerdo con la tabla, $\varphi(9) = 6$.

a	1	2	3	4	5	6	7	8
$\operatorname{mcd}(a,9)$	1	1	3	1	1	3	1	1

Tabla 4.1. Unidades de $\mathbb{Z}_9$: $\varphi(9) = 6$.

Teorema 4.6

p es primo si y solo si $\varphi(p) = p - 1$

Prueba: Si p es primo, los enteros $1,2,...,p-1$ son primos relativos con p y menores que p, entonces $\varphi(p) = p - 1$.
Hay exactamente $p-1$ enteros positivos inferiores a p. Como $\varphi(p) = p - 1$, ninguno de estos $p-1$ enteros divide a p, es decir, p es primo.

Corolario 4.2 *Sea m es compuesto, $\varphi(m) < m - 1$.*

Prueba: Ejercicio.

Teorema 4.7

Sea p primo y $\alpha > 1$. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$

Prueba: Observemos que el conjunto $\{1,2,...,p^\alpha\}$ tiene p^α elementos. Por ejemplo, el conjunto $\{1,2,3,...,5^2\}$ tiene $5^2 = 25$ elementos.

Como p es primo, los números que dividen a p^α e inferiores a él (excepto 1) son los $p^{\alpha-1}$ números

$$p,\, 2p, \ldots, p^{\alpha-1}p.$$

Entonces, en el conjunto $\{1,2,\ldots,p^\alpha\}$ hay $p^\alpha - p^{\alpha-1}$ elementos coprimos con p^α.

Ejemplo 4.10

$\varphi(9) = \varphi(3^2) = 3 \cdot 2 = 6$ y $\varphi(4) = \varphi(2^2) = 2 \cdot 1 = 1$

Si φ fuera multiplicativa, es decir, si $\varphi(nm) = \varphi(n)\varphi(m)$ cuando $\text{mcd}\,(m,n) = 1$, entonces $\varphi(36) = \varphi(2^2 \cdot 3^2) = \varphi(2^2)\varphi(3^2) = 2 \cdot 6 = 12$. Y efectivamente, φ es multiplicativa. Para tener una guía para la demostración de este hecho, necesitamos un lema previo y un ejemplo numérico.

Lema 4.2

Sean $\text{mcd}\,(n,m) = 1$ y r un entero, entonces $\mathbb{Z}_m = \{r,\, n+r,\, 2n+r,\, ...,\, (m-1)n+r\}$

Prueba: Solo necesitamos probar que los m elementos de $A = \{r,\, n+r,\, 2n+r,\, ...,\, (m-1)n+r\}$ no se repiten módulo m. En efecto, si

$$jn + r \equiv in + r \ (\text{mod}\ m),\ i \neq j,\ 0 \leq i,j \leq m-1;$$

entonces, como $\text{mcd}\,(n,m) = 1$, se obtiene $j \equiv i\ (\text{mod}\ m)$, pero esto no puede pasar i y j están en clases distintas módulo m.

Ejemplo 4.11

Sea $n = 4$ y $m = 9$. $\text{mcd}\,(4,9) = 1$. Para establecer una guía para la demostración de que φ es multiplicativa, hacemos un arreglo con los números 1,2,...,36,

$$\begin{bmatrix} 1 & 5 & 9 & 13 & 17 & 21 & 25 & 29 & 33 \\ 2 & 6 & 10 & 14 & 18 & 22 & 26 & 30 & 34 \\ 3 & 7 & 11 & 15 & 19 & 23 & 27 & 31 & 35 \\ 4 & 8 & 12 & 16 & 20 & 24 & 28 & 32 & 36 \end{bmatrix}$$

La idea es eliminar números hasta que nos quede un arreglo rectangular $\varphi(n) \times \varphi(m)$.

La fila i es $i \quad n+i \quad 2n+i \quad \ldots \quad (m-1)n+i$. Como 2 no es primo relativo con $n = 4$, entonces 2 ni la fila $2 \quad n+2 \quad 2n+2 \quad \ldots \quad (m-1)n+2$ es prima relativa con $n = 4$, así que podemos quitar esta fila y, con el mismo argumento, podemos quitar la fila 4.

$$\begin{bmatrix} 1 & 5 & 9 & 13 & 17 & 21 & 25 & 29 & 33 \\ \square & \square & \square & \square & \square & \square & \square & \square & \square \\ 3 & 7 & 11 & 15 & 19 & 23 & 27 & 31 & 35 \\ \square & \square & \square & \square & \square & \square & \square & \square & \square \end{bmatrix}$$

Las filas que quedan son las filas que inician con primos relativos de $n=4$, es decir quedan $\varphi(n)=2$ filas.

Ahora quitamos, en cada fila, los números que no son primos relativos con $m=9$, resulta que los elementos que se deben quitar son $\varphi(m)=3$ elementos:

$$\begin{bmatrix} 1 & 5 & \square & 13 & 17 & \square & 25 & 29 & \square \\ \square & \square & \square & \square & \square & \square & \square & \square & \square \\ 3 & 7 & 11 & \square & 19 & 23 & \square & 31 & \square \\ \square & \square & \square & \square & \square & \square & \square & \square & \square \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 5 & 13 & 17 & 25 & 29 \\ 3 & 7 & 11 & 19 & 23 & 31 \end{bmatrix}$$

En cada fila quedan $\varphi(m)$ elementos, pues si hacemos reducción módulo m, por el lema anterior, la fila $\{i,\ n+i\ 2n+i\ ...\ (m-1)n+i\}$ se convierte en $\{0,2,...,m-1\}$, y en este conjunto solo hay $\varphi(m)$ elementos primos relativos con m. Finalmente el arreglo queda $\varphi(n)\varphi(m)$. Recordemos que si $\operatorname{mcd}(i,n)=1$ y $\operatorname{mcd}(i,m)=1$, entonces $\operatorname{mcd}(i,mn)=1$. Así, el arreglo tiene todos los primos relativos con mn e inferiores a mn, es decir $\varphi(nm)$.

Teorema 4.8

φ es multiplicativa, i.e., si $\operatorname{mcd}(m,n)=1 \implies \varphi(nm)=\varphi(n)\varphi(m)$

Prueba: Consideremos el arreglo

$$\begin{bmatrix} 1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\ \dots & & & & \\ i & m+i & 2m+i & \dots & (n-1)m+i \\ \dots & & & & \\ m-1 & & & & \\ m & 2m & 3m & \dots & mn \end{bmatrix}$$

Si $\operatorname{mcd}(i,n)\neq 1$, entonces los elementos de la fila i no son primos relativos con n. Si quitamos estas filas, quedan $\varphi(n)$ filas

$$r_j \quad n+r_j \quad 2n+r+j \quad ... \quad (m-1)n+r_j,\ j=1,...,\varphi(n)$$

con $\operatorname{mcd}(r_j,n)=1$. Ahora, como $\mathbb{Z}_m=\{r_j,\ n+r_j,\ 2n+r+j,\ ...,\ (m-1)n+r_j\}$, entonces en cada fila de estas solo hay $\varphi(m)$ números primos relativos con m. Finalmente nos queda un arreglo de $\varphi(n)\times\varphi(m)$ con números ambos primos relativos con n y m y por tanto, primos relativos con nm. Como todos son inferiores a nm, $\varphi(nm)=\varphi(n)\varphi(m)$.

El teorema (4.8) nos permite calcular $\varphi(n)$ de manera directa, si conocemos la factorización prima de n,

$$\varphi(n) = \varphi\left(\prod_{i=1}^k p_i^{\alpha_i}\right) = \prod_{i=1}^k p_i^{\alpha_i - 1}(p_i - 1).$$

Teorema 4.9

Sea $n = \prod_{i=1}^k p_i^{\alpha_i}$, p_i primo. Entonces

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Prueba: Si $n = p^\alpha$, $\varphi(n) = \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(p - \frac{1}{p}\right) = n\left(p - \frac{1}{p}\right)$.

Si $n = \prod_{i=1}^k p_i^{\alpha_i}$,

$$\varphi(n) = \varphi\left(\prod_{i=1}^k p_i^{\alpha_i}\right) = \prod_{i=1}^k p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right) = n\prod_{i=1}^k\left(1 - \frac{1}{p_i}\right)$$

Este teorema parece algo extraño, ¿para qué usar fracciones si podemos calcular $\varphi(n)$ con enteros?. Es cierto. Pero esta forma de expresar φ será de mucha utilidad más adelante cuando aparezcan los factores $1 - 1/p_i$ en productos infinitos.

Ejemplo 4.12

Muestre que $\varphi(n) = n/2 \iff n = 2^\alpha$.

Solución: Si $n = 2^\alpha$ el resultado es directo. En la otra dirección, si $n = \prod_{i=1}^k p_i^{\alpha_i}$ y $\varphi(n) = n/2$, entonces $\varphi(n) = n\prod_{i=1}^k(1 - 1/p_i) = n/2$, es decir, $\prod_{i=1}^k(1 - 1/p_i) = 1/2$, por tanto $k = 1$ y $p_1 = 2$, sino tendríamos una contradicción pues si $k > 1$, entonces $\prod_{i=1}^k(1 - 1/p_i) < 1/2$. Finalmente, $n = 2^\alpha$

Por ahora, vamos a establecer un lema análogo al lema (4.1): $a^{\varphi(m)} \equiv 1 \pmod{m}$ si $\operatorname{mcd}(a, m) = 1$. Para familiarizarnos, veamos primero un ejemplo.

Ejemplo 4.13

$\varphi(12) = 4$ cuenta los primos relativos con 12 que son inferiores a 12, es decir $1, 5, 7, 11$.

Ahora, $\operatorname{mcd}(12, 35) = 1$ y $35 \cdot 1 \equiv 11 \pmod{12}$, $35 \cdot 5 \equiv 7 \pmod{12}$, $35 \cdot 7 \equiv 5 \pmod{12}$ y $35 \cdot 11 \equiv 1 \pmod{12}$.

Así, $\{35 \cdot 1, 35 \cdot 5, 35 \cdot 7, 35 \cdot 11\}$ es una permutación módulo 12 de $\{1, 5, 7, 11\}$

El conjunto de unidades de $\mathbb{Z}_m$ se denota $(\mathbb{Z}/m\mathbb{Z})^*$. Este conjunto es un ejemplo de un "sistema reducido de residuos."

Es claro entonces que $|(\mathbb{Z}/m\mathbb{Z})^*| = \varphi(m)$ y, en particular, $|(\mathbb{Z}/m\mathbb{Z})^*| = m-1$ si y solo si m es primo.

Lema 4.3

Sea m entero positivo y $\operatorname{mcd}(a,m)=1$. Sean $r_1, r_2, \ldots, r_{\varphi(m)}$ los $\varphi(m)$ enteros positivos $< m$ y primos relativos con m. Entonces el conjunto de residuos $R = \{\operatorname{rem}(a \cdot r_j, m) \ : \ j = 1,\ldots,\varphi(m)\}$ es una permutación módulo m de los enteros $r_1, r_2, \ldots, r_{\varphi(m)}$.

Prueba: Como el conjunto de residuos $R = \{\operatorname{rem}(a \cdot r_j, m) \ : \ j = 1,\ldots,\varphi(m)\} \subseteq \{r_1, r_2, \ldots, r_{\varphi(m)}\}$, solo hay que demostrar que R tiene $\varphi(m)$ elementos distintos y todos primos relativos con m. Así, estos $\varphi(m)$ números son inferiores a m y coprimos con m, entonces constituyen una permutación módulo m de $r_1, r_2, \ldots, r_{\varphi(m)}$.

Pimero observemos que cada $r_i \in \{1,2,\ldots,m-1\}$ y son todos distintos, por tanto si $i \neq j$; r_i y r_j están en clases de equivalencia distintas y no pueden ser congruentes.

Sea $i \neq j$ con $i,j \in \{1,\ldots,\varphi(m)\}$. Si $a \cdot r_i \equiv a \cdot r_j \pmod{m}$ entonces, como $\operatorname{mcd}(a,m)=1$, podemos cancelar a y nos queda $r_i \equiv r_j \pmod{m}$, pero esto no puede pasar.

Si $\operatorname{mcd}(a \cdot r_i, m) > 1$ entonces sea p un divisor primo de $a \cdot r_i$ y de m. Si $p | a \cdot r_i$, entonces $p | r_i$ o $p | a$. Pero esto no puede pasar pues si $p | r_i$, como $p | m$ entonces contradice el hecho de que $\operatorname{mcd}(r_i, m) = 1$. Por otra parte $p | a$ contradice el hecho de que $\operatorname{mcd}(a,m)=1$.

De nuevo, vamos a dar un ejemplo antes de enunciar el teorema de Euler.

Ejemplo 4.14

$\varphi(12) = 4$ cuenta los primos relativos con 12 que son inferiores a 12, es decir $1,5,7,11$.

Ahora, $\operatorname{mcd}(12,35) = 1$ y $35 \cdot 1 \equiv 11 \pmod{12}$, $35 \cdot 5 \equiv 7 \pmod{12}$, $35 \cdot 7 \equiv 5 \pmod{12}$ y $35 \cdot 11 \equiv 1 \pmod{12}$.

Luego,

$$\begin{aligned} 35^4(1 \cdot 5 \cdot 7 \cdot 11) &\equiv (35 \cdot 1)(35 \cdot 5)(35 \cdot 7)(35 \cdot 11) \pmod{12} \\ &\equiv (11 \cdot 7 \cdot 5 \cdot 1) \pmod{12} \\ \therefore \ 35^4 &\equiv 1 \pmod{12} \end{aligned}$$

pues $\text{mcd}(11 \cdot 7 \cdot 5 \cdot 1, 12) = 1.$

Teorema 4.10 (Teorema de Euler).

Sea m entero positivo y $\text{mcd}(a, m) = 1$, entonces

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Prueba: Sean $r_1, r_2, \ldots, r_{\varphi(m)}$ $\varphi(m)$ los enteros positivos $\leq m$ y primos relativos con m. Entonces, por el lema (4.3),

$$\begin{aligned} a^{\varphi(m)}(r_1 \cdot r_2 \cdots r_{\varphi(m)}) &\equiv (a \cdot r_1)(a \cdot r_2) \cdots (a \cdot r_{\varphi(m)}) \pmod{m} \\ &\equiv (r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)}) \pmod{m} \\ \therefore\ a^{\varphi(m)} &\equiv 1 \pmod{m} \end{aligned}$$

pues $\text{mcd}(r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)}, m) = 1.$

Ejemplo 4.15

$$\begin{aligned} \varphi(6566304875) &= \varphi(5^3 \cdot 13^2 \cdot 310831) \\ &= 5^2(5-1) \cdot 13(13-1) \cdot (310831-1) \\ &= 4848948000. \end{aligned}$$

$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8, \quad \text{pues} \quad \text{mcd}(3,5) = 1.$$

Ejemplo 4.16

Calcular $\text{Ord}_{39}(4)$.

Solución: Como $\varphi(39) = 24$, $\text{Ord}_{39}(4) | 24$. Por tanto, debemos probar solo con los divisores d_i de 24 hasta que $4^{d}_{i} \equiv 1 \pmod{39}$.

$$\begin{aligned} 4 &\equiv \text{rem}(4,39) \\ 4^2 &\equiv \text{rem}(16,39) \\ 4^3 &\equiv \text{rem}(25,39) \\ 4^6 &\equiv \text{rem}(1,39) \end{aligned}$$

$\text{Ord}_{39}(4) = 6$.

4.3.1 Un recíproco del Teorema pequeño de Fermat

Esta es la versión de E. Lucas del recíproco del Teorema pequeño de Fermat: Si p es primo, $\varphi(p) = p-1$ y si p no es primo $\varphi(p) < p-1$. Entonces si $n-1$ es el más pequeño entero positivo tal que $a^{n-1} \equiv 1 \pmod{n}$, n debería ser primo.

Teorema 4.11

Si existe un entero a primo relativo con n tal que $a^{n-1} \equiv 1 \pmod{n}$ y si $a^s \not\equiv 1 \pmod{n}$, para todo $s < n-1$, entonces n es primo.

Prueba: De acuerdo a la hipótesis del teorema, $\text{Ord}_n(a) = n-1$. Si n no fuera primo, $\varphi(n) < n-1$, pero $a^{\varphi(n)} \equiv 1 \pmod{n}$, contradicción con la definición de orden de un número.

Una versión refinada es

Teorema 4.12

Si a y n son enteros primos relativos tales que tales que $a^{n-1} \equiv 1 \pmod{n}$ y $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ para todos los divisores primos q de $n-1$, entonces n es primo.

Prueba: Como los divisores propios de $n-1$ dividen $(n-1)/q$ para algún primo q, entonces $\text{Ord}_m(a)$ no divide al entero $(n-1)/q$, según la hipótesis del teorema. Por tanto, la única posibilidad es que $\text{Ord}_m(a) = n-1$. Así, $(\mathbb{Z}/n\mathbb{Z})^*$ tiene $n-1$ elementos, entonces n debe ser primo.

Con este teorema podríamos decidir si n es primo si conocemos la factorización de $n-1$.

Ejemplo 4.17

Usar el teorema (4.12) para probar que $n = 229$ es primo.

Solución: $n-1 = 2^2 \cdot 3 \cdot 19$. Para probar que n es primo debemos encontrar $2 \leq a \leq 228$ tal que $a^{228} \equiv 1 \pmod{229}$ y $a^{(228)/q} \not\equiv 1 \pmod{229}$ para $q = 2,3,19$. Ahora hacemos una búsqueda exhaustiva:

a	rem$(a^{n-1},229)$	rem$(a^{(n-1)/2},229)$	rem$(a^{(n-1)/3},229)$	rem$(a^{(n-1)/19},229)$
2	1	228	1	203
3	1	1	134	161
4	1	1	1	218
5	1	1	94	61
6	1	228	134	165

Tabla 4.2. $n = 229$ es primo según el teorema (4.12).

$\therefore$ $n = 229$ cumple las condiciones del teorema (4.12) para $a = 6$. Por tanto, $n = 229$ es primo.

4.4 Teorema de Wilson

Sean n, r enteros no negativos. Recordemos que $0! = 1$ y si $n \geq r$, $\binom{n}{r} = \frac{n!}{r!(n-r)!}$. Se puede probar que $\binom{n}{r}$ es un entero procediendo por inducción y usando la identidad de Pascal: $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$

El teorema del binomio establece que si $x,y \in \mathbb{R}$ y n no negativo,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Se asume como convenio que $0^0 = 1$ para el caso especial $x \neq 0$, $y = 0$, $n = 0$.

Teorema 4.13

Si p es primo y $0 < r < p$, entonces $p \,\Big|\, \binom{p}{r}$

Prueba: $\binom{p}{r}$ es un entero así que $r!(p-r)!|p!$. Como $p \nmid r!$ y $p \nmid ((p-r)!)$, entonces $p \nmid r!(p-r)!$. Así $r!(p-r)!|p! \wedge \text{mcd}(p, r!(p-r)!) = 1 \implies r!(p-r)!|(p-1)!$.

$$\therefore \binom{p}{r} = p \cdot \frac{(p-1)!}{r!(p-r)!}.$$

Teorema 4.14

Si p es primo, entonces $(x+y)^p \equiv x^p + y^p \pmod{p}$ si $x, y \in \mathbb{Z}$.

Prueba: Como $p \,\Big|\, \binom{p}{r}$ si $r = 1, 2, \ldots, p-1$, entonces

$$\begin{aligned}(x+y)^p &\equiv \binom{p}{0} y^p + \binom{p}{1} x^1 y^{p-1} + \cdots + \binom{p}{p-1} x^{p-1} y^1 + \binom{p}{p} x^p \pmod{p} \\ &\equiv 1 \cdot y^p + 0 + \cdots + 0 + 1 \cdot x^p \pmod{p}\end{aligned}$$

En general, si p es primo, entonces $(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \pmod{p}$ si $x_i \in \mathbb{Z}$.

Teorema 4.15

Sea p primo y $P(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ con $a_n \not\equiv 0 \pmod{p}$. Entonces la ecuación $P(x) \equiv 0 \pmod{p}$ tiene a lo sumo n soluciones (enteras) distintas módulo p.

Prueba: La prueba es por inducción sobre el grado de P..

Si $n = 0$ no hay soluciones pues $a_0 \not\equiv 0 \pmod{p}$.

Si $n = 1$, la congruencia $a_1 x + a_0 \equiv 0 \pmod{p}$ tiene una solo solución (módulo p) pues $a_1 x \equiv -a_0 \pmod{p}$ tiene solución única módulo p si $\operatorname{mcd}(a_1, p) = 1$.

Supongamos que el resultado es cierto para polinomios de grado $\leq n-1$. Para el resto de la prueba vamos a razonar por contradicción: Supongamos que $P(x) = a_n x^n + \cdots + a_1 x + a_0$ tiene $s > n$ soluciones $a_1, a_2, \ldots, a_s$ distintas módulo p. Consideremos ahora

$$Q(x) = P(x) - a_n (x - a_1)(x - a_2) \cdots (x - a_n).$$

Observe que Q es de grado $\leq n-1$ pues

$$Q(x) = P(x) - a_n (x - a_1)(x - a_2) \cdots (x - a_n) = a_n x^n + \ldots - (a_n x^n + \ldots)$$

y tiene al menos n raíces pues $Q(x) \equiv 0 \pmod{p}$ si $x = a_1, x = a_2, \ldots, a_n$. Por hipótesis de inducción, como Q tiene grado $n-1$, la única posibilidad es que Q sea el polinomio nulo, es decir, $Q(x) \equiv 0 \pmod{p}$ para toda $x \in \mathbb{Z}$. En particular, $Q(a_s) \equiv 0 \pmod{p}$, Entonces

$$\begin{aligned}Q(a_s) &\equiv P(a_s) - a_n (a_s - a_1)(a_s - a_2) \cdots (a_s - a_n) \pmod{p} \\ &\equiv -a_n (a_s - a_1)(a_s - a_2) \cdots (a_s - a_n) \pmod{p} \\ &\equiv 0 \pmod{p}\end{aligned}$$

Luego, $p|a_n(a_s-a_1)(a_s-a_2)\cdots(a_s-a_n)$ y como $p\nmid a_n$, p divide algún factor (a_s-a_j) con lo que $a_j\equiv a_s \pmod p$ en contradicción con nuestra hipótesis.

Teorema 4.16

Sea p primo. Entonces,

$$x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-p+1) \pmod p$$

Prueba: Como p es primo y como p es coprimo con $1,2,...,p-1$, por el teorema de Euler tenemos, $x^{p-1}\equiv 1 \pmod p$ para $x=1,2,...,p-1$. Entonces, $x^{p-1}-1$ es un polinomio con $p-1$ raíces. Usando el teorema (4.15) tenemos

$$x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-p+1) \pmod p \quad \text{si} \quad x=1,2,...,p-1$$

Pero, como $Q(x)=x^{p-1}-1-(x-1)(x-2)\cdots(x-p+1)$ tiene grado $\leq p-2$ y $p-1$ raíces,

$Q(x)\equiv 0 \pmod p$, es decir,

$$x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-p+1) \pmod p \quad \text{si} \quad x\in\mathbb{Z}$$

Teorema 4.17 (Teorema de Wilson).

p es primo si y solo si $(p-1)!\equiv -1 \pmod p$

Prueba: Si p es primo, por el teorema (4.16),

$$x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-(p-1)) \pmod p \quad \text{para cualquier} \quad x\in\mathbb{Z}.$$

Poniendo $x=0$, $-1\equiv(-1)^{p-1}1\cdot 2\cdots(p-1) \pmod p$. Si p es impar, obtenemos el resultado. Si $p=2$ el resultado es directo.

Si $(p-1)!\equiv -1 \pmod p$ y p tiene un divisor d, $1<d<p$, entonces $d|(p-1)!+1$ pero $d|(p-1)!$ pues $1<d<p$, así que $d|1$, contradicción.

Es claro que no es práctico usar este teorema para verificar si p es o no primo.

4.5 Teorema de Carmichael

El cálculo del orden de un número a puede ser complicado. Algo que nos puede ayudar es saber que este orden es inferior a $\varphi(a)$ y un factor de la función $\lambda(a)$ de Carmichael.

Definición 4.3 (Función de Carmichael).

Sean $p, p_1, p_2, ..., p_s$ primos, la función λ se define así:

$$\left.\begin{array}{rcll} \lambda(1) & = & 1, & \\ \lambda(2) & = & 1, & \\ \lambda(4) & = & 2, & \\ \lambda(2^\alpha) & = & 2^{\alpha-2} & \text{si } \alpha \geq 3, \\ \lambda(p^\alpha) & = & \varphi(p^\alpha) = p^{\alpha-1}(p-1) & \text{si } p_i \geq 3 \text{ y } \alpha \geq 1, \\ \lambda(n) & = & \text{mcm}\,(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_k^{\alpha_k})) & \text{si } n = \prod_{i=1}^k p_i^{\alpha_i} \end{array}\right\}$$

Ejemplo 4.18

$\lambda(1) = 1,\ \lambda(2) = 1,\ \lambda(3) = 2,$ etc.

n	1	2	3	4	5	6	7	8	9	10	100	101	102	103
$\lambda(n)$	1	1	2	2	4	2	6	2	6	4	20	100	16	102

Teorema 4.18 (Teorema de Carmichael).

Sean $a, n \in \mathbb{Z}^+$ y $\text{mcd}\,(a, n) = 1$. Entonces

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

Prueba: $n = \prod_{i=2}^k 2^\alpha p_i^{\alpha_i}$, p_i primo y $\text{mcd}\,(a, n) = 1$. Por la definición de la función λ, se tiene

$$\begin{array}{ll} (1) & a^{\lambda(2^\alpha)} \equiv 1 \pmod{2^\alpha} \\ (2) & a^{\lambda(p_1^{\alpha_1})} \equiv 1 \pmod{p_1^{\alpha_1}} \\ (3) & a^{\lambda(p_2^{\alpha_2})} \equiv 1 \pmod{p_2^{\alpha_2}} \\ & \ldots \\ (k) & a^{\lambda(p_k^{\alpha_k})} \equiv 1 \pmod{p_k^{\alpha_k}} \end{array}$$

Ahora, en la primera congruencia, elevamos a ambos lados a la potencia entera $\lambda(n)/\lambda(2^\alpha)$ y en la congruencia $i-$ésima elevamos a ambos lados a la potencia entera $\lambda(n)/\lambda(p_i^{\alpha_i})$, obtenemos

$$\begin{array}{l} a^{\lambda(n)} \equiv 1 \pmod{2^\alpha} \\ a^{\lambda(n)} \equiv 1 \pmod{p_1^{\alpha_1}} \\ a^{\lambda(n)} \equiv 1 \pmod{p_2^{\alpha_2}} \\ \ldots \\ a^{\lambda(n)} \equiv 1 \pmod{p_k^{\alpha_k}} \end{array}$$

Para concluir, recordemos que si $m_1, m_2, ..., m_k \in \mathbb{Z}^+$ y si $a \equiv b \pmod{m_i}$, $i = 1, 2, ..., k$; entonces $a \equiv b\ (\text{mod mcm}\,(m_1 m_2 \cdots m_k))$. Usando este hecho, podemos concluir que $a^{\lambda(n)} \equiv 1 \pmod{n}$.

¿Se gana algo usando $\lambda(n)$ en vez de $\varphi(n)$? Con un esfuerzo razonablemente pequeño, podemos obtener, en general, mejores resultados con λ.

Ejemplo 4.19

Sea $n = 65520 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$. Entonces $\varphi(n) = 8 \cdot 6 \cdot 4 \cdot 6 \cdot 12 = 13824$ mientras que $\lambda(n) = \text{mcm}\,(4,6,4,6,12) = 12$. Entonces, si $\text{mcd}\,(a,n) = 1$,

$$\begin{aligned} a^{\lambda(n)} &\equiv 1 \pmod{65520} \implies a^{12} \equiv 1 \pmod{65520} \\ a^{\varphi(n)} &\equiv 1 \pmod{65520} \implies a^{13824} \equiv 1 \pmod{65520} \end{aligned}$$

Para encontrar el orden de a, se puede probar con los divisores de 12 en vez de calcular y usar los divisores de 13824

Ejemplo 4.20

Calcular $\text{Ord}_{39}(4)$.

Solución: Como $\lambda(39) = 12$, $\text{Ord}_{39}(4)|12$. Por tanto, debemos probar solo con los divisores d_i de 12 hasta que $4^{d_i} \equiv 1 \pmod{39}$.

$$\left.\begin{array}{rcr} 4 & \equiv & \text{rem}(1,39) \\ 4^2 & \equiv & \text{rem}(16,39) \\ 4^3 & \equiv & \text{rem}(25,39) \\ 4^6 & \equiv & \text{rem}(1,39) \end{array}\right\} \implies \text{Ord}_{39}(4) = 6.$$

Uno de los resultados importantes es: $\lambda(n)$ es el más pequeño entero positivo para tal que $a^{\lambda(n)} \equiv 1 \pmod{m}$ para todo a tal que $\text{mcd}\,(a,m) = 1$ (ver [1]).

$\lambda(n)$ y $\varphi(n)$ si $\text{mcd}\,(a,n) > 1$. El teorema de Euler y Carmichael requieren $\text{mcd}\,(a,n) = 1$. Sin embargo hay una versión útil para el caso en que $\text{mcd}\,(a,n)$ no sea necesariamente 1.

Teorema 4.19

Sea $d = \text{mcd}\,(a,n)$,

$$a^{\varphi(n)+1} \equiv a \pmod{n} \iff \text{mcd}\left(d, \frac{n}{d}\right) = 1.$$

Si n es producto de primos distintos,

$$a^{\lambda(n)+1} \equiv a \pmod{n} \quad \text{para cualquier} \quad a \in \mathbb{Z}.$$

Prueba: Ver ([9], pág. 274).

Ejemplo 4.21

Sea $a = 7$ y $n = 210$, $\operatorname{mcd}(a,n) = 7 > 1$, $\varphi(n) = 48$, $7^{49} \equiv 7 \pmod{210}$ y $\operatorname{mcd}(7,30) = 1$ (también $7^1 \equiv 7 \pmod{210}$, $7^5 \equiv 7 \pmod{210}$, etc.).

Sea $n = 2 \cdot 3 \cdot 5 \cdot 7$, $\lambda(n) = 12$, $2^{13} \equiv 2 \pmod{210}$, $3^{13} \equiv 3 \pmod{210}$, etc.

Sea $n = 2^2 \cdot 5$, en este caso $\lambda(n) = 4$ y $2^5 \not\equiv 2 \pmod{n}$, $3^5 \equiv 3 \pmod{n}, \ldots,$ $6^5 \not\equiv 6 \pmod{n}$, etc.

EJERCICIOS

4.1 Verifique, usando el teorema de Fermat, que $2^{340} \equiv 1 \pmod{11}$.

4.2 Verifique que $2^{340} \equiv 1 \pmod{31}$. **Ayuda:** $2^5 \equiv 1 \pmod{31}$

4.3 Verifique que $\operatorname{mcd}(341,2) = 1$ y $2^{340} \equiv 1 \pmod{341}$. ¿Es 341 primo?

4.4 Verifique que $\varphi(666) = 6 \cdot 6 \cdot 6$

4.5 Consideremos los números de Fermat, $F_n = 2^{2^n} + 1$. Vamos a probar, usando congruencias, que si $n \neq m$, $\operatorname{mcd}(F_n, F_m) = 1$. Para probar esto, vamos a suponer, por contradicción, que $\operatorname{mcd}(F_n, F_m) = d > 1$. Entonces hay un primo p tal que $p | F_n$ y $p | F_m$. Bajo esta suposición,

- **a)** verifique que $2^{2^n} \equiv -1 \pmod{p}$,
- **b)** verifique que $2^{2^{n+1}} \equiv 1 \pmod{p}$.
- **c)** Sea $\operatorname{Ord}_p(2) = 2^s$. ¿Porqué $2^s \leq n+1$?
- **d)** Verifique que $s \not\leq n$. **Ayuda:** considere $2^n = 2^s 2^t$ con $s + t = n$ y obtenga una contradicción con $2^{2^n} \equiv -1 \pmod{p}$.
- **e)** Deduzca que el orden de 2 módulo p es 2^{n+1}
- **f)** Deduzca que el orden de 2 módulo p debería ser también 2^{m+1}
- **g)** ¿Cuál es la contradicción?

4.6 Use el resultado anterior para dar otra prueba de que los primos son un conjunto infinito. **Ayuda:** para cada F_n considere uno de sus divisores primos.

4.7 Sea $\operatorname{mcd}(a,m) = 1$ y $\operatorname{Ord}_m(a) = t$. Si $i, j \in \mathbb{Z}$, $a^i \equiv a^j \pmod{m} \iff i \equiv j \pmod{t}$.

4.8 Muestre que si m es compuesto y $\operatorname{mcd}(a,m) = 1$, entonces $\operatorname{Ord}_m(b) < m - 1$. **Ayuda:** Use el teorema de Euler.

4.9 Muestre que si p es primo y $t \nmid (p-1)$, entonces no pueden haber elementos de orden t en $\mathbb{Z}_p$. **Ayuda:** Use Fermat.

4.10 Sea $\operatorname{Ord}_m(a) = t$. Muestre que $\operatorname{Ord}_m(a^i) = t$ si y solo si $\operatorname{mcd}(i,t) = 1$.

4.11 Calcule $\operatorname{Ord}_{13}(5)$ y $\operatorname{Ord}_{13}(7)$

4.12 Sea $\operatorname{mcd}(a,m) = 1$. Muestre que $\operatorname{Ord}_m(a)$ divide a $\phi(m)$.

4.13 Muestre que si p es primo y $\operatorname{mcd}(a,p) = 1$, entonces $\operatorname{Ord}_p(a) | p - 1$.

4.14 Muestre que si $\text{Ord}_m(a) = t$ y k es cualquier entero positivo, entonces $\text{Ord}_m(a^k) = 1$ si y solo si $\text{mcd}(t,k) = 1$.

4.15 Sean $a = 7$ y $m = 310$.

a) Calcule $\varphi(m)$ y $\lambda(m)$.

b) ¿Se puede afirmar, sin calcular, que $a^{\lambda(m)} \equiv 1 \pmod m$?

c) Obtenga $\text{Ord}_m(a)$ **Ayuda:** solo debe probar con los divisores de $\lambda(m)$.

4.16 Sean $a = 7$ y $m = 210$.

a) ¿Tiene sentido hablar de $\text{Ord}_m(a)$?

b) Calcule s tal que $a^s \equiv a \pmod m$.

4.17 Calcule $\text{Ord}_{2337}(2)$

4.18 Muestre que si p es primo y $\text{Ord}_p(a) = t$, entonces las soluciones, módulo p, de $x^t - 1 \equiv 0 \pmod p$ son $\{1, a, a^2, ..., a^{t-1}\}$. ¿porqué no hay más soluciones módulo p?

4.19 Sea p primo impar. Muestre que si $P(x)$ es un polinomio con coeficientes enteros de grado $n \geq 1$ y coeficiente principal $a_n \not\equiv 0 \pmod p$, entonces hay un polinomio $Q(x) \in \mathbb{Z}[x]$ de grado $0 < m < p$ tal que $P(x) \equiv Q(x) \pmod p$.

4.20 Muestre el teorema "pequeño" de Fermat usando el teorema de Euler.

4.21 Muestre el teorema de Euler usando el teorema de Carmichael.

4.22 Muestre que si n es par entonces $\varphi(2n) = 2\varphi(n)$ y que si n es impar entonces $\varphi(2n) = 2\varphi(n)$. **Ayuda:** Teorema (4.8).

4.23 Calcule $\varphi(25)$ usando el teorema (5.2).

4.24 Factorizar $n = 2337$ y calcular $\varphi(n)$ y $\lambda(n)$

4.25 Calcule las raíces (si hubiera) de $P(x) = x^5 + 1$ módulo 5

4.26 Calcule las raíces (si hubiera) de $P(x) = x^5 - 1$ módulo 5

4.27 Calcule 96^{-1} módulo 97. Luego calcule el resto de dividir 95! por 97. **Ayuda:** Fermat y Wilson.

4.28 Sea p primo impar y $\text{mcd}(a,p) = 1$. Mostrar que $a^{(p-1)/2} \equiv 1 \pmod p$ o $a^{(p-1)/2} \equiv -1 \pmod p$. **Ayuda:** Usar la tercera fórmula notable y el teorema de Fermat.

4.29 Resuelva $7x \equiv 1 \pmod{2^6 \cdot 3 \cdot 5 \cdot 17}$ usando primero el teorema pequeño de Fermat y luego usando el teorema de Carmichael.

4.30 Mostrar que si p es primo, entonces $(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \pmod p$ si $x_i \in \mathbb{Z}$.

4.31 Sean $\text{mcd}(a,b) = 1$ y $S = a^{\varphi(b)} + b^{\varphi(a)}$. Muestre que $S \equiv 1 \pmod{ab}$

4.32 Use el teorema "pequeño" de Fermat para probar que si p es primo y $\text{mcd}(p,n) = 1$ y $p|4n^2 + 1$, entonces $p \equiv 1 \pmod 4$. **Ayuda:** Muestre que $p \not\equiv 3 \pmod 4$ por contradicción: Si $p = 4k + 1$ y si $y = 2n$, $y^2 \equiv -1 \pmod p$ luego, como $\text{mcd}(p,y) = 1$, aplique Fermat.

4.33 Muestre que si p es primo y $\text{mcd}(p,n) = 1$ y $p|n^2 + 1$, entonces $p \equiv 1 \pmod 4$ o $p = 2$.

4.34 Muestre que en $\mathbb{Z}_8$, el polinomio $P(x) = x^2 - 1$ tiene 4 raíces: $x = 1,3,5,7$, es decir, $P(1) \equiv 0 \pmod 8$, etc. ¿Contradice esto el teorema (4.15)?

4.35 Muestre el teorema "pequeño" de Fermat usando el teorema del binomio. **Ayuda:** $x_i = 1$.

4.36 Muestre que si $a \equiv 1 \pmod 2$, entonces $a^2 \equiv 1 \pmod{2^3}$. **Ayuda:** $a = 2h+1$, eleve al cuadrado y observe que $h(h+1)$ es par.

4.37 Muestre que si $a^2 \equiv 1 \pmod{2^3}$ entonces $a^{2^2} \equiv 1 \pmod{2^4}$.

4.38 Use inducción para demostrar que si $\alpha > 2$, entonces $a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$.

4.39 Verifique que si $\alpha > 2$, entonces $a^{\frac{1}{2}\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha}$.

4.40 Muestre que si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, p_i primo; entonces $\lambda(p_i^{\alpha_i}) | \lambda(n)$

4.41 Muestre que $\lambda(n) | \varphi(n)$

4.42 Muestre que $\lambda(n) = \varphi(n)$ si $n = 1, 2, 4, p^\alpha, 2p^\alpha$



5 RAÍCES PRIMITIVAS Y LOGARITMO DISCRETO

5.1 Introducción

Se puede demostrar que si p es primo, existe $b \in \mathbb{Z}$ tal que $\mathbb{Z}_p = \{\mathbb{Z}_p = \{0, b, b^2, ..., b^{p-1}\}$. A b se le llama "raíz primitiva" módulo p. Como cualquier elemento $a \in \mathbb{Z}_p$ debe ser una potencia de b, tiene sentido definir un logaritmo discreto (indicador) que resulta tener propiedades similares al logaritmo usual. Es muy útil en el cálculo de residuos y para resolver algunos tipos de ecuaciones congruenciales. Las raíces primitivas módulo n son usadas a menudo en criptografía.

5.2 Raíces Primitivas

Definición 5.1 (Raíces primitivas).

Sea $m \in \mathbb{Z}^+$ y $\operatorname{mcd}(a, m) = 1$. Si $\operatorname{Ord}_m(a) = \varphi(m)$ entonces a se dice raíz primitiva módulo m

Teorema 5.1

Si p es primo y b raíz primitiva módulo p, entonces $\mathbb{Z}_p = \{0, b, b^2, ..., b^{p-1}\}$.

Prueba: Ejercicio.

Ejemplo 5.1

$\text{Ord}_5(3) = 4$ pues $3^2 \equiv 4 \pmod 5$, $3^3 \equiv 2 \pmod 5$ y $3^4 \equiv 1 \pmod 5$. Entonces,

$$\mathbb{Z}_5 = \{\overline{0}, \overline{3}, \overline{3^2}, \overline{3^3}, \overline{3^4}\}$$

Existencia de las raíces primitivas. Para establecer la existencia de las raíces primitivas en cualquier $\mathbb{Z}_p$, p primo; necesitamos algunos resultados.

El teorema que sigue establece que $\sum\limits_{\substack{d|n \\ d>0}} \varphi(d) = n$. Para la demostración, se usa un conjunto $S_d = \{\frac{1}{d}, \frac{2}{d}, \ldots, \frac{d}{d}\}$ y otros conjuntos de fracciones irreducibles (disjuntos):

$$T_d = \left\{ \frac{i}{d} \in S_d \text{ tal que } \text{mcd}\,(i,d) = 1 \right\}.$$

La idea es contar la cantidad de primos relativos como el número de fracciones irreducibles. El siguiente ejemplo muestra la idea de la prueba.

Ejemplo 5.2

Sea $n = 4$. Los divisores positivos de 4 son 1,2,4. Entonces,

$$S_4 = \left\{ \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \frac{4}{4} \right\} \implies |S_4| = 4$$

$$T_4 = \left\{ \frac{1}{4}, \frac{3}{4} \right\} \implies |T_4| = \varphi(4) = 2$$

$$T_2 = \left\{ \frac{1}{2} \right\} \implies |T_2| = \varphi(2) = 1$$

$$T_1 = \left\{ \frac{1}{1} \right\} \implies |T_1| = \varphi(1) = 1$$

Observemos que $T_i \bigcap T_j = \emptyset$ y que $|S_4| = |T_4| + |T_2| + |T_1|$, es decir,

$$4 = \varphi(1) + \varphi(2) + \varphi(4)$$

Teorema 5.2

Sea n un entero positivo, entonces

$$\sum_{\substack{d|n \\ d>0}} \varphi(d) = n$$

Prueba: Sea $S_n = \{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\}$ y sea $T_n = \{\frac{i}{n} \in S_n$ tal que $\text{mcd}\,(i,n) = 1\}$. Claramente $|S_n| = n$ y $|T_n| = \varphi(n)$. Ahora, si $d|n$, $d > 0$; $T_d = \{\frac{i}{d} \in S_d$ tal que $\text{mcd}\,(i,d) = 1\}$, entonces

$$S_n = \bigcup_{\substack{d|n \\ d>0}} T_d = T_1 \cup \ldots \cup T_n$$

En efecto,

"⊆": $\dfrac{i}{n} \in S_n$ tenemos dos casos. Si $\text{mcd}\,(i,n) = 1$, $\frac{i}{n} \in T_n$. Si $\dfrac{i}{n}$ no está en forma reducida, entonces, usando la factorización prima de i y de n, simplificamos y nos queda $\dfrac{i}{n} = \dfrac{k}{h}$ con $\text{mcd}\,(k,h) = 1$ y $1 \leq k \leq h$. Como $h|n$, entonces $\frac{k}{h} \in T_h$ y por tanto está en la unión de los "T_d's".

"⊇": Ahora si $s \in \bigcup_{\substack{d|n \\ d>0}} T_d$, entonces $s \in T_h$ para algún $h|n$. Por tanto, $s = \dfrac{j}{h}$ con $\text{mcd}\,(j,h) = 1$ y $1 \leq j \leq h$. Si $n = k'h$, se tiene $jk' \leq n$, así $s = \dfrac{j}{h} = \dfrac{k'j}{k'h} \in S_n$.

Si d y d' son divisores distintos de n, $T_d \cap T_{d'} = \emptyset$. Esto es así pues si s está en esta la intersección, $s = \dfrac{j}{d} = \dfrac{i}{d'} \implies id = jd'$ y entonces, como $\text{mcd}\,(j,d) = \text{mcd}\,(i,d') = 1$, $d|d'$ y $d'|d$. Esto contradice que $d \neq d'$.

Finalmente, $|S_n| = \sum_{\substack{d|n \\ d>0}} |T_d|$, entonces, como $|T_d| = \varphi(d)$, $n = \sum_{\substack{d|n \\ d>0}} \varphi(d)$.

El teorema (5.2) nos da una fórmula recursiva para calcular $\varphi(n)$. No es un fórmula adecuada para cálculos porque requiere todos los divisores (primos y compuestos) de n

Ejemplo 5.3

Como $\varphi(1) = 1$, $\varphi(3) = 2$ y $\varphi(5) = 4$, entonces

$$\varphi(1) + \varphi(3) + \varphi(5) + \varphi(15) = 15 \implies \varphi(15) = 8.$$

Teorema 5.3

Sea p primo y t un entero positivo. Si $t \nmid (p-1)$ entonces $\mathbb{Z}_p$ no tiene elementos de orden t. Si $t|(p-1)$, hay exactamente $\varphi(t)$ elementos de orden t en $\mathbb{Z}_p$

Prueba: De acuerdo al teorema "pequeño" de Fermat, para cada $a \in \mathbb{Z}_p$, $\overline{a} \neq \overline{0}$, $a^{p-1} \equiv 1 \pmod{p}$. Luego, si a es de orden t, $t|(p-1)$, o lo que es lo mismo, si $t \nmid (p-1)$ no hay elementos de orden t.

Para probar la segunda parte, definimos una nueva función $\psi(t)$: Para cada entero positivo s que divide a $p-1$, sea $\psi(s)$ el número de elementos de orden s en $\mathbb{Z}_p$. Ahora, como cada

elemento en $\mathbb{Z}_p^*$ tiene algún orden s que divide a $p-1$, entonces

$$\sum_{t|(p-1)} \psi(t) = p-1$$

Por el teorema (5.2), $\sum_{t|(p-1)} \varphi(t) = p-1$, entonces

$$\sum_{t|(p-1)} (\varphi(t) - \psi(t)) = 0$$

Pero, para cualquier entero t, no hay elementos de orden t o hay exactamente $\varphi(t)$ elementos de orden t; entonces $\varphi(t) - \psi(t) \geq 0$ para todo t. Como los sumandos son ≥ 0 y la suma da cero, cada sumado vale cero: $\varphi(t) = \psi(t)$ para cada $t|(p-1)$.

Corolario 5.1 *Si p es primo, en $\mathbb{Z}_p$ hay $\varphi(p-1)$ elementos de orden $p-1$, es decir, hay $\varphi(p-1)$ raíces primitivas.*

Ejemplo 5.4

Cuando tenemos un primo pequeño, podemos localizar las raíces primitivas por "ensayo y error", construyendo una tabla de potencias.

a	a^1	a^2	a^3	a^4	a^5	a^6	$\text{Ord}_7(a)$
1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	3
3	3	2	6	4	5	1	6
4	4	2	1	4	2	1	3
5	5	4	6	2	3	1	6
6	6	1	6	1	6	1	2

Tabla 5.1. Potencias de los elementos de $\mathbb{Z}_7$

Solo hay $\varphi(6) = 2$ raíces primitivas módulo 7, 3 y 5 tienen orden 6, es decir, son las únicas dos raíces primitivas módulo 7. También, por ejemplo, $\mathbb{Z}_7 = \{0, 5, 5^2, 5^3, 5^4, 5^5, 5^6\}$.

Ejemplo 5.5

La tabla que sigue es un listado de las raíces primitivas de los primeros seis primos.

p	$\varphi(p-1)$	Raíces primitivas
2	1	1
3	1	2
5	2	2, 3
7	2	3, 5
11	4	2, 6, 7, 8
13	4	2, 6, 7, 11

Tabla 5.2. Raíces primitivas módulo p

Si b es raíz primitiva del primo p, hay $\varphi(p-1)$ raíces primitivas no congruentes, a saber, $b^{\alpha_1}, b^{\alpha_2}, ..., b^{\alpha_{\varphi(p-1)}}$, donde $\alpha_1, \alpha_2, ..., \alpha_{\varphi(p-1)}$ son los $\varphi(p-1)$ enteros menores que $p-1$ y coprimos con $p-1$.

Ejemplo 5.6

Determinar las raíces primitivas de 17 sabiendo que 3 es raíz primitiva módulo 17.

Solución: Como $\varphi(17) = 8$, los ocho enteros menores que 16 y coprimos con 16 son $1,3,5,7,9,11,13$ y 15. Así, la raíces primitivas son $3^3, 3^5, 3^7, 3^9, 3^1 1, 3^1 3$. Haciendo la reducción a módulo 17, no queda $3,10,5,11,14,7,12,6$.

Ya probamos la existencia de raíces primitivas para p primo. El siguiente teorema define la situación general.

Teorema 5.4 (Gauss).

Un entero $n > 1$ tiene raíces primitivas módulo n si y solo si $n = 2,\ 4,\ p^\alpha$ o $2p^\alpha$ donde p es primo impar y α entero positivo.

En particular, todos los primos tienen raíces primitivas.

Ejemplo 5.7

Los primeros n para los que hay raíces primitivas son $2,3,4,5,6,7,9,10,11,13,$ $14,17,18,19,22,....$ En particular, no hay raíces primitivas módulo $n = 2^4 = 16$.

En resumen, podemos determinar si hay o no hay raíces primitivas módulo n y el cálculo de estas raíces se hace usando "prueba y error" (aunque hay unas pocas técnicas generales de cálculo).

5.3 Logaritmo discreto o Indicador

El problema que queremos resolver es el siguiente: Si sabemos que $a \equiv b^k \pmod{m}$, ¿Cómo determinar k?

Recordemos que en $\mathbb{Z}_n$ hay $\varphi(n)$ elementos primos relativos con n.

Definición 5.2 (Sistema reducido de residuos).

Sea $n \in \mathbb{Z}^+$. El conjunto $\{a_1, a_2, ..., a_{\varphi(n)}\}$ es un sistema reducido de residuos módulo n, si contiene exactamente un elemento de cada una de las clases $\overline{r_i} \in \mathbb{Z}_n$ para las que $\text{mcd}\,(r_i, n) = 1$.

Ejemplo 5.8

Si $n = p$ es primo, $\{1, 2, ..., p-1\}$ es un sistema reducido de residuos módulo p.

Si $n = 10$, $\varphi(10) = 4$. En este caso, $\{1, 3, 7, 9\}$ es un sistema reducido de residuos módulo 10.

Claramente, si b es una raíz primitiva módulo n, el conjunto $\{b, b^2, ..., b^{\varphi(n)}\}$ es un sistema reducido de residuos. Entonces, si $a \in \mathbb{Z}_n$ con $\text{mcd}\,(a, n) = 1$, existe $1 \leq k \leq \varphi(n)$ tal que $a \equiv b^k \pmod{n}$. En particular $1 \equiv b^{\varphi(n)} \pmod{n}$, por el teorema de Euler.

Definición 5.3

Sea b una raíz primitiva módulo n. Si $\text{mcd}\,(a, n) = 1$, entonces el más pequeño entero positivo k tal que $a \equiv b^k \pmod{n}$ se denota con $\text{Ind}_b(a)$ y se llama indicador de a respecto a la base b módulo n.

Entonces tenemos,

$$a \equiv b^{\text{Ind}_b(a)} \pmod{n}$$

A veces se pone $\text{Ind}_b(a) = \log_b a$ y se le llama "logaritmo discreto".

Propiedades. Las propiedades de $\text{Ind}_b(a)$ son similares a las de la función logaritmo.

Teorema 5.5

Sea b raíz primitiva módulo n y $\operatorname{mcd}(a,n)=\operatorname{mcd}(c,n)=1$. Entonces,

a.) $b^x \equiv b^y \pmod n \iff x \equiv y \pmod{\varphi(n)}$

b.) $\operatorname{Ind}_b(1) \equiv 0 \pmod{\varphi(n)}$

c.) $\operatorname{Ind}_b(ac) \equiv [\operatorname{Ind}_b(a)+\operatorname{Ind}_b(c)] \pmod{\varphi(n)}$

d.) $\operatorname{Ind}_b(a^k) \equiv k\cdot\operatorname{Ind}_b(a) \pmod{\varphi(n)}$, si k es entero positivo.

Prueba: Ejercicio.

El teorema 5.5 **a.)** nos dice que,

$$a \equiv b^k \pmod n \iff \operatorname{Ind}_b(a) = \operatorname{rem}(k,\varphi(n)) \tag{5.1}$$

La reducción módulo $\varphi(n)$ es necesaria para obtener el menor exponente positivo, excepto cuando $1 \equiv b^{\varphi(n)} \pmod n$, es claro que, como $1 \equiv b^{\varphi(n)} \pmod n$, $\operatorname{Ind}_b(1)=\varphi(n)$.

Ejemplo 5.9

Se sabe que $b=5$ es raíz primitiva módulo 7 y $\varphi(7)=6$,

a.) $2 \equiv 5^{10} \pmod 7 \iff \operatorname{Ind}_5(2) = \operatorname{rem}(10,6) = 4$, es decir, efectivamente $2 \equiv 5^4 \pmod 7$.

b.) $1 \equiv 5^6 \pmod 7 \iff \operatorname{Ind}_5(1) = \operatorname{rem}(6,6)=0$, es decir, como efectivamente indica 5.5 **b.)** , $6=\operatorname{Ind}_5(1) \equiv 0 \pmod 6$.

Observe que el teorema 5.5 nos dice que "Ind" se puede aplicar igual que se aplican los logaritmos para resolver ecuaciones (siempre y cuando se cumplan las hipótesis),

$$g(x) \equiv f(x) \pmod m \implies \operatorname{Ind}_b(g(x)) \equiv \operatorname{Ind}_b(f(x)) \pmod{\varphi(m)}.$$

Por supuesto, la aplicación de esta parte del teorema requiere tener a la mano una tabla de indicadores. En el ejemplo que sigue construimos una breve tabla para $\operatorname{Ind}_2(a)$ módulo 13.

Ejemplo 5.10

Como es usual, para usar el teorema (5.5) necesitamos una tabla de logaritmos discretos. Por ejemplo, para construir una tabla parcial en base $b=2$ módulo 13, calculamos las potencias de 2 módulo 13.

$$\begin{array}{rclrcl} 2 & \equiv & 2^1 \,(\text{mod } 13), & 11 & \equiv & 2^7 \,(\text{mod } 13), \\ 4 & \equiv & 2^2 \,(\text{mod } 13), & 9 & \equiv & 2^8 \,(\text{mod } 13), \\ 8 & \equiv & 2^3 \,(\text{mod } 13), & 5 & \equiv & 2^9 \,(\text{mod } 13), \\ 3 & \equiv & 2^4 \,(\text{mod } 13), & 10 & \equiv & 2^{10} \,(\text{mod } 13), \\ 6 & \equiv & 2^5 \,(\text{mod } 13), & 7 & \equiv & 2^{11} \,(\text{mod } 13), \\ 12 & \equiv & 2^6 \,(\text{mod } 13), & 1 & \equiv & 2^{12} \,(\text{mod } 13). \end{array}$$

Luego, ponemos la información en una tabla,

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{Ind}_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6

Tabla 5.3. Logaritmos discreto base $b = 2$ módulo 13

Ejemplo 5.11

Resolver $8x^5 \equiv 2 \pmod{13}$ con $\text{mcd}\,(x, 13) = 1$

Solución: Como $b = 2$ es raíz primitiva módulo 13 y como conocemos una tabla de logaritmos discretos para esta base, podemos aplicar "$\text{Ind}_2(\cdot)$" a ambos lados de la ecuación $8x^5 \equiv 2 \pmod{13}$,

$$8x^5 \equiv 2 \pmod{13} \Longrightarrow \text{Ind}_2(8x^5) \equiv \text{Ind}_2(2) \pmod{\varphi(13)}$$

Ahora operamos,

$$\begin{array}{rcll} \text{Ind}_2(8x^5) & \equiv & \text{Ind}_2(2)\,(\text{mod}\,\varphi(13)) & \\ \text{Ind}_2(8) + 5\text{Ind}_2(x) & \equiv & 1\,(\text{mod}\,12), & \text{pues } \text{mcd}\,(8,13) = 1 \text{ y } \text{mcd}\,(x,13) = 1, \\ 3 + 5\text{Ind}_2(x) & \equiv & 1\,(\text{mod}\,12), & \text{pues } \text{Ind}_2(8) = 3 \\ 5\text{Ind}_2(x) & \equiv & -2\,(\text{mod}\,12), & \\ \text{Ind}_2(x) & \equiv & -10\,(\text{mod}\,12), & \text{pues } 5 \cdot 5 \equiv 1 \pmod{12} \\ \text{Ind}_2(x) & \equiv & 2\,(\text{mod}\,12), & \text{pues } -10 \equiv 2 \pmod{12} \\ x & \equiv & \text{rem}(2^2, 13), & \text{por } 5.1 \end{array}$$

Y, efectivamente, $8 \cdot 4^5 = 8192 \equiv 2 \pmod{13}$.

Ejemplo 5.12

Resolver $2^{3x} \equiv 8 \pmod{13}$.

Solución: Como $b = 2$ es raíz primitiva módulo 13, podemos aplicar "$\text{Ind}_2(\cdot)$" a ambos lados,

$$\begin{array}{rcl} 2^{3x} \equiv 8 \pmod{13} & \Longrightarrow & \text{Ind}_2(2^{3x}) \equiv \text{Ind}_2(8) \pmod{12} \\ & \Longrightarrow & 3x \equiv 3 \pmod{12} \\ & \Longrightarrow & x \equiv 1 \pmod{4} \end{array}$$

Ahora, los elementos en $\mathbb{Z}_{13}$ que son congruentes con 1 módulo 4 son $x = 1, 5, 9$.

Ejemplo 5.13

Calcule el residuo de dividir $12^{729} \cdot 7^{97}$ por 17.

Solución: 3 es raíz primitiva módulo 17. Así que podemos tomar logaritmo discreto en base 3. En particular, $\text{Ind}_3(12) = 13$ y $\text{Ind}_3(7) = 11$.

Sea $x \equiv 12^{729} \cdot 7^{97} \pmod{17}$, aplicando logaritmo discreto,

$\text{Ind}_3(x) \equiv \text{Ind}_3(12^{729} \cdot 7^{97}) \pmod{16}$,

entonces $\text{Ind}_3(x) \equiv 729 \cdot \text{Ind}_3(12) + 97 \cdot \text{Ind}_3(7) \equiv 9 \cdot 13 + 1 \cdot 11 \equiv 0 \pmod{16}$, es decir, $x \equiv 1$ (mod 17.)

Ejemplo 5.14

Probar que la congruencia $25x^5 \equiv 17 \pmod{71}$ no tiene solución

Solución: Para aplicar logaritmo discreto a ambos lados, necesitamos una raíz primitiva módulo 71. Como $\text{Ord}_{71}(7) = 70$, $g = 7$ es raíz primitiva módulo 71. En particular, $\text{Ind}_7(17) = 49$ y $\text{Ind}_7(25) = 15$. Ahora,

$\text{Ind}_7(25x^5) \equiv \text{Ind}_7(17) \pmod{70} \Leftrightarrow 5 \cdot \text{Ind}_7(x) \equiv \text{Ind}_7(17) - \text{Ind}_7(25) \pmod{70}$, es decir, $5 \cdot \text{Ind}_7(x) \equiv 34 \pmod{70}$.

Esta última congruencia no tiene solución pues $\text{mcd}(5,70) = 5 \nmid 34$.

Comparado con el logaritmo común, el logaritmo discreto tiene dos defectos: (1) las tablas se deben construir para cada módulo primo y hay $\varphi(p-1)$ posibles bases; (2) los datos en las tablas no están en orden ascendente.

El siguiente teorema establece algunas fórmulas útiles para el cálculo de índices.

Teorema 5.6

Sea b una raíz primitiva módulo m.

a.) Si $\text{mcd}(a,m) = 1$, entonces $\text{Ind}_b(a^{-1}) = \varphi(m) - \text{Ind}_b(a)$

b.) Si $m \geq 3$, $\text{Ind}_b(m-1) = \varphi(m)/2$

c.) Si p es primo impar, $\text{Ind}_b(p-1) = \varphi(p-1)/2$

d.) Si $m \geq 3$ y $\text{mcd}(a,m) = 1$, entonces $\text{Ind}_b(m-1) = \text{Ind}_b(a) + \varphi(m)/2$

e.) Si m es primo impar y $\text{mcd}(a,m) = 1$, entonces $\text{Ind}_b(m-1) = \text{Ind}_b(a) + \varphi(m-1)/2$

Ejemplo 5.15

Podemos usar la parte **e.)** del teorema (5.6) para construir una tabla para logaritmo discreto en base 3 módulo 7,

a	1	2	3	4	5	6
$\text{Ind}_3(a)$	6	2	1	.	.	.

Tabla 5.4. Logaritmos discreto base $b = 3$ módulo 7

EJERCICIOS

5.1 Muestre que en $\mathbb{Z}_7$, las únicas raíces primitivas son 3 y 5.

5.2 Calcule las raíces primitivas de módulo 71.

5.3 Muestre que si b es raíz primitiva módulo p y $b \equiv c \pmod p$, entonces c es raíz primitiva módulo p.

5.4 Sea $p = 2^n + 1$. Verifique que si p es primo, entonces n es par **Ayuda:** Solamente puede pasar $p \equiv 2 \pmod 3$. Ahora use logaritmo discreto.

5.5 Verifique que no hay raíces primitivas módulo 8.

5.6 Verifique que 8 no es raíz primitiva módulo 13.

5.7 ¿Hay raíces primitivas en $\mathbb{Z}_{12}$?

5.8 Calcule las raíces primitivas de $\mathbb{Z}_{11}$

5.9 Si p es primo y t un entero, muestre que si en $\mathbb{Z}_p$ hay elementos de orden t, entonces hay exactamente $\varphi(t)$ elementos de este orden.

5.10 Sea p primo y $\text{Ord}_p(a) = t$. Muestre que si $b \in \mathbb{Z}_p$ y $b^t \equiv 1 \pmod p$, entonces b debe ser una potencia de a.

5.11 Construya una tabla para el logaritmo discreto en base 11

5.12 Resolver

a) $7x \equiv 13 \pmod{18}$
b) $2x^4 \equiv 5 \pmod{13}$
c) $8^{5x} \equiv 5 \pmod{13}$

d) $3^{4x+1} \equiv 10 \pmod{19}$

e) $8x^2 \equiv 2 \pmod{13}$. Sugerencia: $x \equiv 2^{\text{Ind}_2(x)} \pmod{13}$ con $\text{Ind}_2(x) \equiv 5 \pmod 6$ y $\text{Ind}_2(x) \in \{1,2,...,12\}$.

5.13 Sea $m = m_1 m_2$ con $\text{mcd}(m_1, m_2) = 1$ y $m_i \geq 3$.

a) Muestre que si $m \geq 3$, $\varphi(m)$ es par

b) Sea $n = \varphi(m_1)\varphi(m_2)/2$ y $\text{mcd}(a, m) = \text{mcd}(a, m_1) = \text{mcd}(a, m_2) = 1$. Muestre que $a^{\varphi(m_1)\varphi(m_2)/2} \equiv 1 \pmod{m_1}$ y que $a^{\varphi(m_2)\varphi(m_1)/2} \equiv 1 \pmod{m_2}$

c) Muestre que $a^n \equiv 1 \pmod{m}$

5.14 Usar logaritmo discreto para encontrar el residuo de dividir 23^{1001} por 13.



6 RESIDUOS CUADRÁTICOS

6.1 Congruencias cuadráticas módulo m

Definición 6.1

Una congruencia cuadrática es una congruencia de la forma

$$x^2 \equiv a \pmod{m}$$

donde $\text{mcd}(a,n) = 1$. Si la congruencia tiene solución, a es llamado *residuo cuadrático* módulo m.

Ejemplo 6.1

Calcular los residuos cuadráticos módulo 7.

Solución: Una manera directa es hacer una tabla de cuadrados,

b	1	2	3	4	5	6	
Residuo $\text{rem}(b^2,7)$	1	4	2	2	4	1	$\longleftarrow$ residuos cuadráticos

Tabla 6.1. Residuos cuadráticos módulo 7

Tenemos,

$$\begin{array}{rcl} 1^2 \equiv 6^2 & \equiv & 1 \pmod{7} \\ 2^2 \equiv 5^2 & \equiv & 4 \pmod{7} \\ 3^2 \equiv 4^2 & \equiv & 2 \pmod{7} \end{array} \implies 1,2,4 \text{ son residuos cuadráticos } \bmod 7.$$

La congruencia $Ax^2 + Bx + C \equiv 0 \pmod{p}$. Observemos que si p es primo y $p \nmid A$; la congruencia $Ax^2 + Bx + C \equiv 0 \pmod{p}$ es equivalente a $(2Ax + B)^2 \equiv B^2 - 4AC \pmod{p}$ (ver ejercicios), o lo que es lo mismo, $u^2 \equiv a \pmod{p}$ con $u = 2Ax + B$ y $a = B^2 - 4AC$.

Representación simétrica. En principio podemos decidir si la congruencia $x^2 \equiv a \pmod{p}$ tiene solución o no, por ensayo y error. La teoría que sigue está orientada a buscar respuestas a preguntas como ¿cuándo es soluble o no, esta congruencia?, si es soluble, ¿cuántas soluciones tiene módulo p?. La teoría requiere trabajar con la representación simétrica de $\mathbb{Z}_p$.

$$\mathbb{Z}_p = \begin{cases} \left\{-\dfrac{p-1}{2}, ..., -1, 0, 1, ...\dfrac{p-1}{2}\right\} & \text{si } p \text{ es impar} \\ \left\{-\dfrac{p-1}{2}+1, ..., -1, 0, 1, ...\dfrac{p-1}{2}\right\} & \text{si } p \text{ es par} \end{cases}$$

En las aplicaciones, el caso común es cuando p es impar. La regla de conversión para pasar de $\{0, 1, ..., p-1\}$ a representación simétrica es sencilla:

$$\begin{cases} i \longrightarrow i & \text{si } 0 \leq i \leq \dfrac{p-1}{2}, \\ \dfrac{p-1}{2}+k \longrightarrow -\dfrac{p-1}{2}+k-1 & \text{con } 1 \leq k \leq \dfrac{p-1}{2}. \end{cases}$$

Ejemplo 6.2

Consideremos $\mathbb{Z}_7$, $\dfrac{p-1}{2} = 3$.

$$\begin{array}{ccccccc} 0, & 1, & 2, & 3, & 4, & 5, & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0, & 1, & 2, & 3, & -3, & -2, & -1 \end{array}$$

Si volvemos a calcular como en el ejemplo (6.1), pero esta vez usando la representación simétrica, se nos hará evidente nuestro siguiente teorema,

b	-3	-2	-1	1	2	3	
$\text{rem}(b^2, 7)$	2	4	1	1	4	2	$\longleftarrow$ residuos cuadráticos mod 7

Tabla 6.2. Residuos cuadráticos módulo 7

Tenemos,

$$\begin{aligned} (-1)^2 \equiv 1^2 &\equiv 1 \pmod 7 \\ (-2)^2 \equiv 2^2 &\equiv 4 \pmod 7 \\ (-3)^2 \equiv 3^2 &\equiv 2 \pmod 7 \end{aligned}$$

Teorema 6.1

Sea p primo impar y $\text{mcd}\,(a, p) = 1$.

a.) $x^2 \equiv a \pmod p$ no tiene solución o tiene exactamente dos soluciones mod p,

b.) Hay exactamente $\dfrac{p-1}{2}$ residuos cuadráticos $\text{rem}(1^2, p)$, $\text{rem}(2^2, p)$, ..., $\text{rem}(\left(\dfrac{p-1}{2}\right)^2, p)$ y $\dfrac{p-1}{2}$ residuos no cuadráticos.

Prueba: **a.)** Si $x^2 \equiv a \pmod{p}$ y $y^2 \equiv a \pmod{p}$ entonces $p|x^2-y^2 \implies p|x+y \vee p|x-y \implies x \equiv \pm y \pmod{p}$.

b.) Sea $\mathbb{Z}_p = \{-(p-1)/2,...,-1,0,1,...,(p-1)/2\}$. Entonces tenemos $(p-1)/2$ residuos cuadráticos a_j con $(-j)^2 = j^2 \equiv a_j \pmod{p}$, $-(p-1)/2 \leq j \leq (p-1)/2$ y $j \neq 0$. Claramente son residuos cuadráticos distintos pues si $i \not\equiv j \pmod{p}$ entonces $i^2 \not\equiv j^2 \pmod{p}$ si $i,j \in \{1,...,(p-1)/2\}$ (ya que $0 < |i-j| < i+j < p-1$). Hay exactamente $(p-1)/2$ residuos cuadráticos pues ya agotamos los cuadrados en $\mathbb{Z}_p$.

En el caso $p=2$ el teorema no aplica: sólo hay un residuo cuadrático módulo $2:\ 1^2 \equiv 1 \pmod{2}$.

6.2 Criterio de Euler

Euler divisó un criterio sencillo, para decidir si un número es residuos cuadrático módulo p. El criterio no es muy práctico computacionalmente pero si de gran valor teórico.

La idea es la siguiente: Si a es residuo cuadrático módulo p, hay un entero x tal que $a \equiv_p x^2$, entonces, por el teorema pequeño de Fermat se tiene

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p},$$

es decir, si a es residuo cuadrático módulo p,

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Ejemplo 6.3

Sea $p=11$. Vamos a calcular todas las potencias $a^{(p-1)/2}$ módulo p en representación estándar y en representación simétrica,

a	1	2	3	4	5	6	7	8	9	10	
Residuo rem$(a^{(p-1)/2}, p)$	1	10	1	1	1	10	10	10	1	10	← estándar
Residuo rem$_s(a^{(p-1)/2}, p)$	1	−1	1	1	1	−1	−1	−1	1	−1	← simétrica

Teorema 6.2 (Criterio de Euler).

Sea p primo impar y $\text{mcd}\,(a,p)=1$, entonces

a.) a es residuo cuadrático $\iff a^{(p-1)/2} \equiv 1 \pmod{p}$,
b.) a no es residuo cuadrático $\iff a^{(p-1)/2} \equiv -1 \pmod{p}$,

Prueba: Para la demostración usamos el teorema pequeño de Fermat y logaritmo discreto.

La parte **a.)** requiere probar dos dos direcciones,

$'' \Longrightarrow ''$ Si a es un residuo cuadrático módulo p, existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod{p}.$ Como $\text{mcd}(a,p) = 1$ entonces $\text{mcd}(x^2,p) = 1$. Ahora aplicamos el teorema pequeño de Fermat,

$$\begin{aligned} 1 &\equiv x^{p-1} \,(\text{mod}\, p) \\ &\equiv (x^2)^{(p-1)/2} \,(\text{mod}\, p) \\ &\equiv a^{(p-1)/2} \,(\text{mod}\, p) \end{aligned}$$

$'' \Longleftarrow ''$ Si $a^{(p-1)/2} \equiv 1 \pmod{p}$, sea b una raíz primitiva de p (todos los primos tienen raíces primitivas) y sea $t \in \mathbb{Z}$ tal que $a \equiv b^t \pmod{p}$. Entonces,

$$\begin{aligned} & b^t &\equiv\;& a \,(\text{mod}\, p) \\ \Longrightarrow\;& b^{t(p-1)/2} &\equiv\;& a^{(p-1)/2} \equiv 1 \,(\text{mod}\, p) \\ \Longrightarrow\;& \text{Ind}_b(b^{t(p-1)/2}) &\equiv\;& \text{Ind}_b(1) \equiv 0 \,(\text{mod}\, p) \\ \Longrightarrow\;& t(p-1)/2 &\equiv\;& 0 \,(\text{mod}\,(p-1)) \\ \Longrightarrow\;& t(p-1) &=\;& 2k(p-1),\; k \in \mathbb{Z},\; \text{ i.e. } t \text{ es par.} \\ \Longrightarrow\;& \left(b^{t/2}\right)^2 &=\;& b^t \equiv a \pmod{p},\; \text{ i.e. } a \text{ es residuo cuadrático módulo } p. \end{aligned}$$

b.). Para probar esta parte se suficiente observar que, por el Pequeño Teorema de Fermat,

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Como p es primo, no hay divisores de cero en $\mathbb{Z}_p$, por lo que si a no es residuo cuadrático módulo p, la única opción que queda es $a^{(p-1)/2} \equiv -1 \pmod{p}$. La otra implicación es consecuencia de la parte **a.)**

El criterio de Euler, en su versión cruda, es útil en el cálculo directo si p es pequeño, dado que tenemos que calcular la potencia $a^{(p-1)/2}$.

Ejemplo 6.4

¿Es $a = 72$ residuo cuadrático módulo 229?

Solución: Tenemos que calcular $\text{rem}(72^{114}, 229)$. Para simplificar el cálculo descomponemos en potencias de 2,

$72^{114} = 72^2 \cdot ((((72^2)^2)^2)^2)^7 \equiv 228 \equiv -1 \text{ mod } 229$; no es residuo cuadrático.

Ejemplo 6.5

Sea p primo impar. Muestre que si b es raíz primitiva módulo p, entonces b no es residuo cuadrático módulo p.

Solución: Como $\text{Ord}_p(b) = p-1$, entonces $b^{(p-1)/2} \not\equiv 1 \pmod p$ y por el criterio de Euler, la única posibilidad es que $b^{(p-1)/2} \equiv -1 \pmod p$, es decir, b no es residuo cuadrático módulo p.

6.3 Símbolos de Legendre y Jacobi

El símbolo de Legendre nos permite establecer si un número a es o no es residuo cuadrático módulo un primo p, mediante un cálculo automático. La ley de la reciprocidad cuadrática, una de las joyas de la teoría de números, simplifica notablemente este cálculo.

El símbolo de Jacobi es una generalización del símbolo de Legendre que permite una simplificación del cálculo cuando el módulo no es primo.

Los estudios en residuos cuadráticos de Euler fueron extendidos por Legendre. El símbolo de Legendre nos proporciona una serie de reglas para el cálculo automático. Estas reglas en el fondo, son aplicaciones simplificadas del criterio de Euler.

Definición 6.2

Sea p un primo impar y $\text{mcd}\,(a,p) = 1$. El símbolo de Legendre $\left(\dfrac{a}{p}\right)$ es definido por,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ residuo cuadrático módulo } p \\ -1 & \text{si } a \text{ no es residuo cuadrático módulo } p \end{cases}$$

En algunos textos se usa una definición alternativa: Si p es primo impar,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ residuo cuadrático módulo } p \\ 0 & \text{si } p|a \\ -1 & \text{si } a \text{ no es residuo cuadrático módulo } p \end{cases}$$

Ejemplo 6.6

Los residuos cuadráticos de $\mathbb{Z}_7$ son 1,2,4, es decir, $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$ y $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$

Para el cálculo del símbolo de Legendre es necesario establecer las siguientes propiedades,

Teorema 6.3

Sea p primo impar y $mcd(p,a) = \text{mod}(p,b) = 1$. Entonces,

a.) $\left(\frac{a}{p}\right) = \text{rem}_s(a^{(p-1)/2}, p)$ (rem_s es el residuo en representación simétrica).

b.) $\left(\frac{a^2}{p}\right) = 1$. En particular $\left(\frac{1}{p}\right) = 1$.

c.) Si $a \equiv b \pmod{p}$ entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, En particular, $\left(\frac{a}{p}\right) = \left(\frac{\text{rem}(a,p)}{p}\right)$.

d.) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

e.) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4} \\ -1 & \text{si } p \equiv -1 \pmod{4} \end{cases}$

Prueba: El item **a.)** es el criterio de Euler: $a^{(p-1)/2} \equiv 1 \pmod{p}$ o $a^{(p-1)/2} \equiv -1 \pmod{p}$. Entonces $\text{rem}_s(a^{(p-1)/2}, p) = \pm 1$ y el signo depende de que a sea residuo cuadrático o no.

b.): Sea $r_a = \text{rem}_s(a^2, p)$. Entonces $\text{mcd}\,(r_a, p) = 1$ y $a^2 \equiv r_a \pmod{p}$, es decir, $\left(\frac{a^2}{p}\right) = 1$.

c.): $a \equiv b \pmod{p} \implies a^{(p-1)/2} \equiv b^{(p-1)/2} \pmod{p}$. Luego, por **a.)**, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

d.): Como $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ y $b^{(p-1)/2} \equiv \pm 1 \pmod{p}$, entonces $(ab)^{(p-1)/2} \equiv \pm 1 \pmod{p}$ y entonces el signo de $\text{rem}_s((ab)^{(p-1)/2}, p) = \pm 1$ depende de los signos de $\text{rem}_s(a^{(p-1)/2}, p)$ y $\text{rem}_s(b^{(p-1)/2}, p)$ por separado. En resumen, aplicando **a.)**,

$$\begin{aligned} \left(\frac{ab}{p}\right) &= \text{rem}_s((ab)^{(p-1)/2}, p) \\ &= \text{rem}_s(a^{(p-1)/2} b^{(p-1)/2}, p) \\ &= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \end{aligned}$$

e.): Por **a.)**

$$\left(\frac{-1}{p}\right) \equiv \text{rem}_s((-1)^{(p-1)/2}, p) = (-1)^{(p-1)/2} \quad \text{(en representación simétrica)}$$

Ahora, como $p \in \mathbb{Z}_4$ y p es primo impar, entonces las únicas posibilidades son: $p \equiv 1 \pmod 4$ o $p \equiv 3 \pmod 4$. Si $p = 4k+1$ para algún entero k, $(p-1)/2 = 2k =$ par. Si $p = 4k-1$ para algún entero k, $(p-1)/2 = 2k-1 =$ impar. Por lo tanto,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4 \\ -1 & \text{si } p \equiv -1 \pmod 4 \end{cases}$$

Corolario 6.1 *Sea p primo impar,*

a.) *Sea* $\text{mcd}\,(n, p) = 1$. *Si* $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ *es la descomposición prima de* n,

$$\left(\frac{\prod_{i=1}^{k} p_i^{\alpha_i}}{p}\right) = \prod_{i=1}^{k} \left(\frac{p_i}{p}\right)^{\alpha_i}$$

b.) *El producto de dos residuos cuadráticos módulo p es residuo cuadrático módulo p.*

c.) *El producto de dos residuos no cuadráticos módulo p es residuo cuadrático módulo p.*

d.) *El producto de un residuo cuadrático y otro no cuadrático módulo p, es un residuo no cuadrático módulo p.*

Prueba: Ejercicio.

Ejemplo 6.7

$$\left(\frac{2}{5}\right) = \text{rem}_s(2^{(5-1)/2}, 5) = \text{rem}_s(4, 5) = -1 \text{ por el teorema 6.3 **a.)**.}$$

Ejemplo 6.8

El criterio de Euler, bajo el símbolo de Legendre, nos da un criterio rápido para decidir si $a = -1$ es o no es residuo cuadrático módulo p.

a.) $a = -1$ no es residuo cuadrático módulo 3 pues $\left(\frac{-1}{3}\right) = (-1)^{(3-1)/2} = -1$

b.) $a=-1$ es residuo cuadrático módulo 229 pues $\left(\frac{-1}{229}\right)=(-1)^{(229-1)/2}=(-1)^{114}=1.$

Ejemplo 6.9

En este ejemplo vamos a aver como se aplican algunas de las propiedades del símbolo de Legendre.

a.) ¿Es 10 residuo cuadrático del primo 3?

Solución: $\left(\frac{-10}{3}\right)=\left(\frac{-1}{3}\right)\left(\frac{10}{3}\right)=\left(\frac{1}{3}\right)=-1$ por el teorema (6.3), **c.)**.

b.) ¿Es 63 residuo cuadrático del primo 11?

Solución:

$$\begin{aligned}
\left(\frac{63}{11}\right) &= \left(\frac{8}{11}\right) && \text{por (6.3), \textbf{c.)}}\\
&= \left(\frac{2}{11}\right)\left(\frac{2^2}{11}\right) && \text{por (6.3), \textbf{d.)}}\\
&= \left(\frac{2}{11}\right)\cdot 1 && \text{por (6.3), \textbf{a.)}}\\
&= -1\cdot 1 && \text{por cálculo directo.}
\end{aligned}$$

por tanto 63 no es residuo cuadrático módulo 11.

Ejemplo 6.0 (continuación).

c.) ¿Es 72 residuo cuadrático del primo 229?

Solución: Por el corolario (6.1),

$$\left(\frac{72}{229}\right)=\left(\frac{2^3\cdot 3^2}{229}\right)=\left(\frac{2}{229}\right)^3\left(\frac{3}{229}\right)^2=1\cdot\left(\frac{2}{229}\right)\cdot 1=-1$$

Ejemplo 6.10

Probar que hay una cantidad infinita de primos de la forma $4k+1$.

Solución: Por contradiccón, supongamos que solo hay una cantidad finita $P = \{p_1, p_2, ..., p_s\}$ de primos de la forma $4k+1$. Sea $N = (2p_1 p_2 \cdots p_s)^2 + 1$. Observemos que si $p_i \in P$, $N = k' p_i + 1$, es decir, los p_i's no dividen N. Como N es de la forma $4k+1$ y no es un p_i, es compuesto. Entonces sería divisible por un primo $p \notin P$. Por tanto, -1 es residuo cuadrático módulo p y p debería ser de la forma $4k+1$. Contradicción.

6.3.1 Lema de Gauss

El lema de Gauss es una herramienta teórica que al igual que el criterio de Euler, nos provee de método para calcular el símbolo de Legendre vía un conteo de signos.

La idea es la siguiente: Si p es primo impar y $\operatorname{mcd}(a,p) = 1$, entonces

$$\mathbb{Z}_p = \{0, a \cdot 1, a \cdot 2, ..., (p-1) \cdot a\}$$

Los números $a \cdot 1, a \cdot 2, ..., a \cdot \dfrac{p-1}{2}$ son distintos módulo p. Si consideramos $\mathbb{Z}_p$ en representación simétrica, tenemos

$$\{a \cdot 1, a \cdot 2, ..., a \cdot \frac{p-1}{2}\} \subseteq \left\{-\frac{p-1}{2}, ..., -1, 0, 1, ..., \frac{p-1}{2}\right\}$$

Por ejemplo, si $p = 13$ y $a = 3$, tenemos

$3 \cdot i$	$3 \cdot 1$	$3 \cdot 2$	$3 \cdot 3$	$3 \cdot 4$	$3 \cdot 5$	$3 \cdot 6$
$\operatorname{rem}(3 \cdot i, 13)$	3	6	-4	-1	2	5

Tabla 6.3. Representación simétrica de $3 \cdot i$, $i = 1, ..., 6$

En representación simétrica los números aparecen con una copia positiva y otra negativa, es decir, aparece el 1 y el -1, el 2 y el -2, etc. Pero, al pasar cada elemento del conjunto $\{a \cdot i,\ i = 1, ..., (p-1)/2\}$ a representación simétrica, solo aparece una copia: aparece el 1 o el -1, el 2 o el -2, etc.

Ahora, sacando a factor común a y los signos, tenemos

$$a^{(p-1)/2} \cdot 1 \cdot 2 \cdots \frac{p-1}{2} (-1)^{\omega} = a \cdot 1 \cdot a \cdot 2 \ldots a \cdot \frac{p-1}{2} \equiv 1 \cdot 2 \cdots \frac{p-1}{2} \bmod p,$$

por tanto, cancelando: $a^{(p-1)/2} \equiv (-1)^{\omega} \pmod p$. Así, el número ω de signos "$-$" en $\{a \cdot, a \cdot 2, ..., a \cdot \dfrac{p-1}{2}\}$ define si a es residuo cuadrático o no.

Lema 6.1 (Lema de Gauss).

Sea p primo impar y $\text{mcd}(a,p) = 1$. Si ω es la cantidad de enteros en el conjunto

$$\{a \cdot 1 \bmod p,\, a \cdot 2 \bmod p, ...,\, a \cdot \frac{p-1}{2} \bmod p\}$$

que son más grandes que $(p-1)/2$ (negativos en representación simétrica), entonces

$$\left(\frac{a}{p}\right) = (-1)^{\omega}$$

Prueba: : Sea $R = \{\, \text{rem}(a,\, p),\ \text{rem}(2 \cdot a,\, p),\ ...,\ \text{rem}(\frac{p-1}{2} \cdot a\,,\, p)\}$. En R no hay elementos congruentes pues $\text{mcd}(a,p) = 1$. Vamos a denotar con $r_1, r_2, ..., r_k$ los elementos de R que son $\leq (p-1)/2$ y $s_1, s_2, ..., s_\omega$ los elementos de R que son $> (p-1)/2$. Por tanto, $k + \omega = (p-1)/2$.

Los $(p-1)/2$ enteros $r_1, r_2, ..., r_k, p - s_1, p - s_2, ..., p - s_\omega$ son positivos y $\leq (p-1)/2$. Todos estos números son distintos módulo p : En efecto, ya conocemos que $r_1, r_2, ..., r_k, s_1, s_2, ..., s_\omega$ son distintos módulo p, como $s_i \not\equiv s_j \pmod p$ entonces $p - s_i \not\equiv p - s_j \pmod p$. También $p - s_i \not\equiv r_j \pmod p$ si $i \neq j,\, 1 \leq i,j \leq (p-1)/2$; para probarlo, supongamos que $p - s_i \equiv r_j \pmod p$, entonces $-s_i \equiv r_j \pmod p \implies s_i + r_j \equiv 0 \pmod p$ pero esto es imposible pues $0 < s_i + r_j \leq (p-1)/2$. Esto demuestra que

$$\{r_1, r_2, ..., r_k, p - s_1, p - s_2, ..., p - s_\omega\} = \{1, 2, ..., (p-1)/2\}.$$

Entonces

$$\begin{aligned}
1 \cdot 2 \cdots (p-1)/2 &\equiv r_1 \cdot r_2 \cdots r_k \cdot (p - s_1) \cdot (p - s_2) \cdots (p - s_\omega) \pmod p \\
&\equiv r_1 \cdot r_2 \cdots r_k \cdot -s_1 \cdot -s_2 \cdots - s_\omega \pmod p, \quad \text{pues} \quad p \equiv 0 \\
&\qquad \text{sacamos los } \omega \text{ signos ``}-\text{'' a factor común,} \\
&\equiv (r_1 \cdot r_2 \cdots r_k \cdot s_1 \cdot s_2 \cdots s_\omega)(-1)^{\omega} \pmod p, \\
&\equiv (a \cdot 1 \cdot a \cdot 2 \cdots a \cdot (p-1)/2)(-1)^{\omega} \pmod p, \\
&\qquad \text{sacamos } a \text{ a factor común,} \\
&\equiv (a^{(p-1)/2}(1 \cdot 2 \cdots (p-1)/2)(-1)^{\omega} \pmod p, \\
&\qquad \text{cancelamos,} \\
1 &\equiv a^{(p-1)/2}(-1)^{\omega} \pmod p, \quad \text{es decir,} \\
a^{(p-1)/2} &\equiv (-1)^{\omega} (\text{mod } p).
\end{aligned}$$

Ahora, por el criterio de Euler, $\left(\frac{a}{p}\right) = (-1)^{\omega}$.

Nota: En la práctica, en vez de contar los signos negativos, contamos los residuos $\text{rem}(a \cdot i,\, p) > p/2$. Usamos $p/2$ en vez de $(p-1)/2$ pues

$$\frac{p-1}{2} < \frac{p}{2} < \frac{p-1}{2} + 1 = \frac{p+1}{2}.$$

El siguiente ejemplo ilustra el cálculo. Recordemos que la importancia del lema es de orden teórico no computacional.

Ejemplo 6.11

¿Es $a = 63$ residuo cuadrático módulo $p = 11$?

Solución: $\{63 \cdot i,\ i = 1,...,5\} = \{8,5,2,10,7\}$. Hay $\omega = 3$ números $> [\![p/2]\!] = 5$. Por tanto $\left(\dfrac{63}{11}\right) = (-1)^3 = -1$. $\therefore$ 63 no es residuo cuadrático módulo 11.

Ya sabemos cómo decidir si ± 1 es residuo cuadrático módulo p. Podemos aplicar el lema de Gauss para decidir si 2 es residuo cuadrático módulo p.

Teorema 6.4

Si p es primo impar, entonces

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod 8 \\ -1 & \text{si } p \equiv \pm 3 \pmod 8 \end{cases} \tag{6.1}$$

En particular, si a es par, $\left(\dfrac{a}{p}\right) = (-1)^{(p^2-1)/8}\left(\dfrac{a/2}{p}\right)$.

Prueba: Para calcular $\left(\dfrac{2}{p}\right)$ contamos los números en $\{2 \cdot i,\ i = 1,...,(p-1)/2\}$ tales que $2 \cdot i > p/2$, es decir, $i > p/4$ (aquí no hay que hacer reducción módulo p pues $0 \le 2i \le p-1$). Entonces $2i > p/2$ si $[\![p/4]\!] < i \le (p-1)/2$. Por lo tanto,

$$\omega = \frac{p-1}{2} - \left[\!\!\left[\frac{p}{4}\right]\!\!\right].$$

Esto nos da

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/2 - \left[\!\left[\frac{p}{4}\right]\!\right]}$$

Aquí lo que interesa es saber si $(p-1)/2 - [\![\frac{p}{4}]\!]$ es par o impar, así que hacemos una reducción módulo 2 :

$$\frac{p-1}{2} - \left[\!\!\left[\frac{p}{4}\right]\!\!\right] \equiv \frac{p^2-1}{8} \pmod 2. \tag{6.2}$$

Para probar esto último usamos el hecho de que, como p es primo impar, $\exists\, k \in \mathbb{Z}$ tal que $p = 8k + r$ con $r = 1, -1, 3$ o -3. Luego,

$$\left[\!\!\left[\frac{p}{4}\right]\!\!\right] = \begin{cases} 2k & \text{si } r = 1 \\ 2k-1 & \text{si } r = -1 \\ 2k & \text{si } r = 3 \\ 2k-1 & \text{si } r = -3 \end{cases}$$

En estos cuatro casos se cumple (6.2) y además si $r = \pm 1$, $\dfrac{p^2-1}{8}$ es par y si $r = \pm 3$, $\dfrac{p^2-1}{8}$ es impar.

Aquí solo vamos a probar los casos $r = 3$ y $r = -1$, los otros casos son similares.

Si $p = 8k + 3$, entonces

$$\frac{p-1}{2} - \left[\!\left[\frac{p}{4}\right]\!\right] = 1 + 4k - 2k = 1 + 4k \equiv 1 \pmod 2$$

$$\frac{p^2-1}{8} = 1 + 6k + 8k^2 \equiv 1 \pmod 2. \text{ Esto prueba (6.2) para este caso.}$$

$$\text{Como } \frac{p^2-1}{8} \text{ es impar, } \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = -1 \text{ si } p \equiv 3 \pmod 8$$

Si $p = 8k - 1$, entonces

$$\frac{p-1}{2} - \left[\!\left[\frac{p}{4}\right]\!\right] = 4k - 1 - (2k-1) = 2k \equiv 0 \pmod 2$$

$$\frac{p^2-1}{8} = -2k + 8k^2 \equiv 0 \pmod 2. \text{ Esto prueba (6.2) para este caso.}$$

$$\text{Como } \frac{p^2-1}{8} \text{ es par, } \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = 1 \text{ si } p \equiv -1 \pmod 8.$$

La idea de la congruencia es muy útil: es más fácil verificar la congruencia que calcular la potencia.

Ejemplo 6.12

a.) ¿Es 2 residuo cuadrático módulo 97?

Solución: Sí, $\left(\frac{2}{97}\right) = 1$ pues $97 \equiv 1 \pmod 8$

b.) ¿Es 2 residuo cuadrático módulo 229?

Solución: No, $\left(\frac{2}{97}\right) = -1$ pues $229 \equiv 3 \pmod 8$

6.3.2 Ley de Reciprocidad Cuadrática.

La ley de reciprocidad cuadrática establece una sorprendente relación entre $\left(\frac{p}{q}\right)$ y $\left(\frac{q}{p}\right)$. Esta ley fue conjeturada, basándose en evidencia numérica, por Euler en 1783 y Lagrange en 1785. Legendre le dio la forma actual a esta ley, pero no pudo dar una prueba completa. La primera prueba rigurosa fue dada por Gauss en a la edad de 18 años. Hasta el 2004 se conocían 190

pruebas diferentes. Gauss llamó a este teorema "Aureum Theorema". Su importancia en la teoría de números no tienen discusión. Al respecto, Hecke afirmó al respecto: "La teoría de números moderna comenzó con el descubrimiento de la Ley de Reciprocidad Cuadrática".

La prueba del teorema sigue es la tercera prueba que dio Gauss. La prueba se basa e un argumento geométrico.

Primero veamos un ejemplo concreto. Sea $p = 11$ y $q = 7$. El número $\left[\!\left[\frac{4 \cdot q}{p}\right]\!\right] = 2$ cuenta la cantidad de números $\leq \frac{4 \cdot q}{p}$. Geométricamente corresponde a la cantidad de pares ordenados con componentes enteros (llamados *punto reticulares*) sobre la parte positiva de la recta $x = 4$ y por debajo de la recta $y = \frac{q}{p}x$. Estos puntos son de la forma $(4, y)$ con $y \leq \frac{4 \cdot q}{p}$.

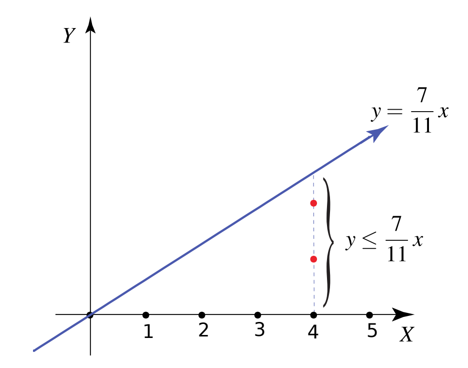


Tabla 6.4. Puntos reticulares $(4, y)$ con $y \leq 4 \cdot 11/7$

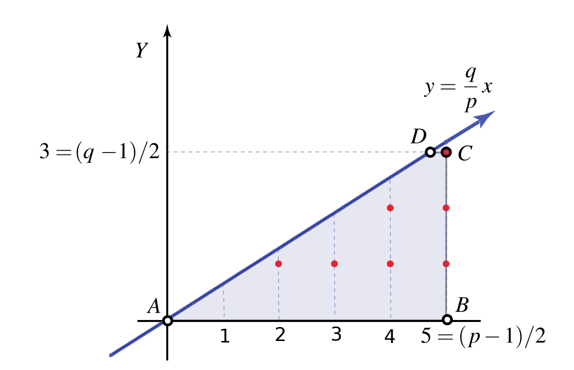


Tabla 6.5. Puntos reticulares en $ABCD$

La suma $\displaystyle\sum_{k=1}^{(p-1)/2} \left[\!\left[\frac{k \cdot q}{p}\right]\!\right] = 7$ corresponde a los puntos reticulares en el polígono $ABCD$ de la figura (6.5).

Podemos cambiar el punto de vista y ver las cosas desde el eje Y de una manera totalmente simétrica: El número $\left[\!\left[\frac{3 \cdot p}{q}\right]\!\right] = 4$ cuenta la cantidad de números $\leq \frac{3 \cdot p}{q}$. Geométricamente corresponde a la cantidad de de puntos reticulares sobre la parte derecha de la recta $y = 3$ y por debajo de la recta $x = \frac{p}{q}y$. Estos puntos son de la forma $(x, 3)$ con $x \leq \frac{3 \cdot p}{q}$.

La suma $\displaystyle\sum_{k=1}^{(q-1)/2} \left[\!\left[\frac{k \cdot p}{q}\right]\!\right] = 8$ corresponde a los puntos reticulares en el polígono $APQR$ de la figura (6.1).

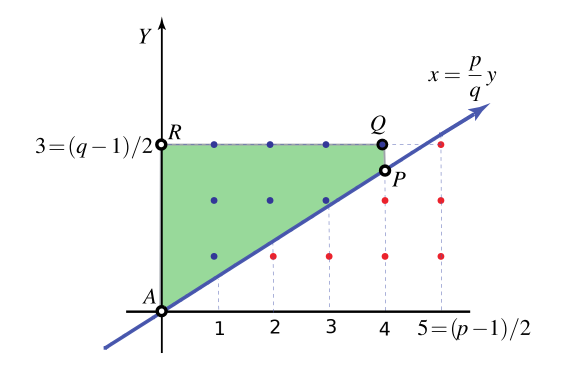


Figura 6.1. Puntos reticulares en $APQR$

Finalmente, la figura (6.1) también nos sugiere que

$$\sum_{k=1}^{(p-1)/2} \left[\!\left[\frac{k \cdot q}{p}\right]\!\right] + \sum_{k=1}^{(q-1)/2} \left[\!\left[\frac{k \cdot p}{q}\right]\!\right] = 7 + 8 = 15 = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Observemos además, que si $p > q$ entonces $\left[\!\left[\frac{q}{p}\frac{p-1}{2}\right]\!\right] = \frac{q-1}{2}$. La prueba se puede hacer de manera directa y está en los ejercicios. Note que, por simetría, si $q > p$, entonces $\left[\!\left[\frac{p}{q}\frac{q-1}{2}\right]\!\right] = \frac{p-1}{2}$.

Ahora que hemos establecido el significado geométrico de estas sumas, consideremos el siguiente lema,

Lema 6.2

Sean p, q primos impares distintos. Entonces,

$$\sum_{k=1}^{(p-1)/2} \left[\!\left[\frac{k \cdot q}{p}\right]\!\right] + \sum_{k=1}^{(q-1)/2} \left[\!\left[\frac{k \cdot p}{q}\right]\!\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Prueba: Sea $p > q$. El número $[\![k \cdot q/p]\!]$ cuenta la cantidad de números $\leq (k \cdot q)/p$. Geométricamente corresponde a la cantidad de puntos reticulares sobre la parte positiva de la recta $x = k$ y por debajo de la recta $y = q/p\,x$. Estos puntos son de la forma (k,y) con $y \leq k \cdot q/p$.

Cuando $x = (p-1)/2$, la cantidad de puntos es $y = (q-1)/2$ pues

$$\frac{q-1}{2} \leq \frac{q}{p}\frac{p-1}{2} < \frac{q-1}{2} + 1.$$

La suma $S(p,q) = \sum_{k=1}^{(p-1)/2} [\![k \cdot q/p]\!]$ corresponde a la suma de los puntos reticulares en el polígono $ABCD$ de la figura (6.2).

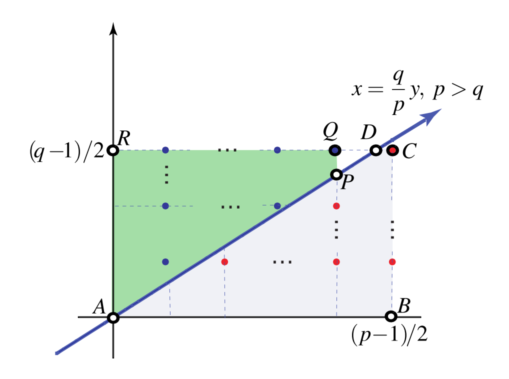


Figura 6.2. Puntos reticulares

De manera simétrica, la suma $S(q,p) = \sum_{k=1}^{(q-1)/2} [\![k \cdot p/q]\!]$ corresponde a la suma de los puntos reticulares en el polígono $APQR$ de la figura (6.2).

Hay que notar que no hay puntos reticulares sobre la recta $y = \frac{q}{p}x$ pues $\operatorname{mcd}(p,q) = 1$.

Finalmente, la suma de los puntos reticulares en el polígono $ABCR$ se puede expresar de dos formas: $\frac{p-1}{2} \cdot \frac{q-1}{2}$ y $S(q,p) + S(p,q)$.

Teorema 6.5 (Ley de Reciprocidad Cuadrática).

Sea p y q primos impares distintos. Entonces

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

En particular, $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$.

Prueba: Sea $R = \{\operatorname{rem}(q,p), \operatorname{rem}(2\cdot q,p), ..., \operatorname{rem}(\frac{p-1}{2}\cdot q,p)\}$. Vamos a denotar con $r_1, r_2, ..., r_k$ los elementos de R que son $\leq p/2$ y $s_1, s_2, ..., s_\omega$ los elementos de R que son $> p/2$. Claramente $k + \omega = (p-1)/2$ y $\left(\frac{q}{p}\right) = (-1)^\omega$.

Los elementos de R son todos distintos. Si $i, j \in R$ y $i \neq j$, entonces $i \not\equiv p - j \pmod p$. Así, los $(p-1)/2$ números $r_1, r_2, ..., r_k, p - s_1, p - s_2, ..., p - s_\omega$ son todos distintos e inferiores a $p/2$, por tanto estos números corresponden a los números $1, 2, ..., (p-1)/2$ en algún orden. Entonces

$$\begin{aligned} \sum_{i=1}^{k} r_k + \sum_{i=1}^{\omega}(p - s_i) &= \sum_{i=1}^{(p-1)/2} i \\ &= \frac{(p-1)(p+1)}{8} \end{aligned}$$

Por tanto,

$$\sum_{i=1}^{k} r_k + \sum_{i=1}^{\omega}(p - s_i) = \sum_{i=1}^{k} r_k + \omega p - \sum_{i=1}^{\omega} s_i = \frac{p^2-1}{8}$$

Sea $S(p,q) = \sum_{k=1}^{(p-1)/2} [\![k \cdot q/p]\!]$, $S_1 = \sum_{i=1}^{k} r_k$ y $S_2 = \sum_{i=1}^{\omega} s_i$. Con esta notación,

$$\frac{p^2-1}{8} = S_1 + \omega \cdot p - S_2 \tag{6.3}$$

Por el algoritmo de la división,

$$kq = [\![kq/p]\!] \cdot p + t_k \quad \text{con} \quad 0 \leq t_k < p.$$

Entonces,

$$\sum_{k=1}^{(p-1)/2} k \cdot q = \sum_{k=1}^{(p-1)/2} [\![kq/p]\!] \cdot p + \sum_{k=1}^{(p-1)/2} t_k.$$

Esto es,

$$\begin{aligned} q \cdot \sum_{k=1}^{(p-1)/2} k &= p \cdot S(p,q) + S_1 + S_2 \\ q \cdot \frac{p^2-1}{8} &= p \cdot S(p,q) + S_1 + S_2 \end{aligned} \tag{6.4}$$

Ahora restando (6.3) con (6.4) obtenemos,

$$(q-1) \cdot \frac{p^2-1}{8} = p \cdot (S(p,q) - \omega) + 2S_2$$

De aquí se sigue que $S(p,q) - \omega$ es par. Por tanto, $(-1)^{S(p,q)-\omega} = 1$; es decir $(-1)^{S(p,q)} = (-1)^{\omega}$. Pero, el lema de Gauss dice que $\left(\frac{q}{p}\right) = (-1)^{\omega}$, entonces $\left(\frac{q}{p}\right) = (-1)^{S(p,q)}$. De manera similar, $\left(\frac{p}{q}\right) = (-1)^{S(q,p)}$. En conclusión,

$$\begin{aligned} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{S(q,p)} \cdot (-1)^{S(p,q)} \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}, \quad \text{por el lema de Gauss.} \end{aligned}$$

El corolario que sigue es una reformulación de la Ley de Reciprocidad Cuadrática en términos de congruencias.

Corolario 6.2 *Sea p y q primos impares distintos. Entonces*

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{si } \; p \equiv 1 \pmod 4 \; \text{ o } \; q \equiv 1 \pmod 4 \\ \left(\frac{p}{q}\right) & \text{si } \; p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Prueba: Ejercicio.

Ejemplo 6.13

¿Es 152 residuo cuadrático módulo 43?

Solución: $152 \equiv 23 \pmod{43}$, entonces

$$
\begin{aligned}
\left(\frac{153}{43}\right) &= \left(\frac{23}{43}\right) \\
&= -\left(\frac{43}{23}\right), \quad \text{pues} \quad 43 \equiv 23 \equiv 3 \pmod 4, \quad \text{(Corolario 6.2)} \\
&= -\left(\frac{20}{23}\right), \quad \text{pues} \quad 43 \equiv 20 \pmod{23} \\
&= -\left(\frac{2^2}{23}\right) \cdot \left(\frac{5}{23}\right) = -\left(\frac{5}{23}\right) \\
&= -\left(\frac{23}{5}\right) \quad \text{pues} \quad 5 \equiv 1 \pmod 4 \\
&= -\left(\frac{2}{5}\right) = -1 \quad \text{pues} \quad \left(\frac{2}{5}\right) = (-1)^{(25-1)/8} = 1.
\end{aligned}
$$

Ejemplo 6.14

Muestre que si $p = 2^n + 1$ es primo $\Longrightarrow 3$ es raíz primitiva módulo p.

Solución: $p \not\equiv 1 \pmod 3$ y, como p es primo, $p \not\equiv 0 \pmod 3$. Así, $p \equiv 2 \pmod 3$. Por tanto, $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$. Ahora, por el criterio de Euler, $3^{2^{n-1}} \equiv -1 \pmod p$ y también $3^{2^n} \equiv 1 \pmod p$. Sea ahora $\text{Ord}_p(3) = s$, entonces $s | 2^n \Rightarrow s = 2^k$ con $k \leq n$. Si $k < n$, entonces

$$1 \equiv \left(3^{2^k}\right)^{2^{n-k-1}} \equiv 3^{2^{n-1}} \equiv -1 \pmod p,$$

lo cual es una contradicción. $\therefore$ 3 es raíz primitiva.

Ejemplo 6.15

Sea p primo > 3. Muestre que si $p \equiv 1 \pmod 4$ y $p \equiv 1 \pmod 3$ entonces $\left(\frac{3}{p}\right) = 1$

Solución: Por la Ley de Reciprocidad Cuadrática,

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$$

y como $p = 4k+1$, entonces,

$$\left(\frac{3}{p}\right) = (-1)^{2k}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Ahora, como $p \equiv 1 \pmod 3$ entonces

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$$

6.4 Símbolo de Jacobi.

El símbolo de Jacobi es una extensión del símbolo de Legendre pero solo decide si un número es un residuo *no* cuadrático. La notación es la misma, el símbolo de Jacobi se denota $\left(\frac{a}{m}\right)$ solo que esta vez m debe ser impar y $\text{mcd}\,(a,m) = 1$. No hay peligro de confusión pues si m es primo impar, el símbolo de Jacobi coincide con el símbolo de Legendre. Si m no es primo, estamos en el contexto del símbolo de Jacobi.

Definición 6.3 (Símbolo de Jacobi).

Sea m entero positivo impar con descomposición prima $m = \prod_{i=1}^{k} p_i^{e_i}$, y sea a entero tal que $\text{mcd}\,(a,m) = 1$. El símbolo de Jacobi se define por

$$\left(\frac{a}{m}\right) = \left(\frac{a}{\prod_{i=1}^{k} p_i^{e_i}}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{e_i}$$

En esta definición, formalmente $\left(\frac{a}{p_i}\right)$ corresponde al símbolo de Legendre.

Ejemplo 6.16

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1 \text{ (aunque } 2 \text{ \textit{no} es residuo cuadrático módulo 15!)}$$

- Si m es primo, el símbolo de Jacobi coincide con el símbolo de Legendre.
- Si m no es primo, el símbolo de Jacobi no decide si a es residuo cuadrático módulo m: 2 no es residuo cuadrático módulo 15 pero, usando el símbolo de Jacobi, $\left(\frac{2}{15}\right) = 1$.

- El símbolo de Jacobi si decide residuos no cuadráticos. Si $\left(\dfrac{a}{m}\right) = -1$, a no es residuo cuadrático módulo m. Esto es así pues si $\left(\dfrac{a}{m}\right) = -1$, entonces por definición, si m es compuesto, hay un divisor primo impar p_i de m tal que $\left(\dfrac{a}{p_i}\right) = -1$. Si suponemos que a es residuo cuadrático módulo m tendríamos una contradicción pues $x^2 \equiv a \pmod{m} \implies x^2 \equiv a \pmod{p_i}$.

- El símbolo de Jacobi simplifica el cálculo del símbolo de Legendre cuando a es compuesto impar y p primo, como veremos más adelante.

Teorema 6.6 Propiedades del símbolo de Jacobi

Sea m un entero positivo impar, a,b,n enteros con $\operatorname{mcd}(a,m) = \operatorname{mcd}(b,m) = 1$ entonces,

a.) $\left(\dfrac{a}{m}\right) = \left(\dfrac{\operatorname{rem}(a,m)}{m}\right)$

b.) $\left(\dfrac{ab}{m}\right) = \left(\dfrac{a}{m}\right)\left(\dfrac{b}{m}\right)$

c.) $\left(\dfrac{a^2}{m}\right) = 1$. En particular, $\left(\dfrac{1}{m}\right) = 1$

d.) $\left(\dfrac{-1}{m}\right) = (-1)^{(m-1)/2}$

e.) $\left(\dfrac{2}{m}\right) = (-1)^{(m^2-1)/8}$

f.) Ley generalizada de reciprocidad cuadrática. $\left(\dfrac{n}{m}\right) = \left(\dfrac{m}{n}\right)(-1)^{(m-1)(n-1)/4}$ si también n es impar y $\operatorname{mcd}(m,n) = 1$

Ejemplo 6.17

$\left(\dfrac{391}{439}\right)$ corresponde al símbolo de Legendre pues 439 es primo. Como $\operatorname{mcd}(391,439) = 1$, podemos usar la ley generalizada de reciprocidad cuadrática calculando como símbolo de Jacobi.

$$\begin{aligned}
\left(\frac{391}{439}\right) &= (-1)^{(439-1)(391-1)/4}\left(\frac{439}{391}\right) \quad \text{(Reciprocidad cuadrática generalizada)}\\
&= -1\cdot\left(\frac{439}{391}\right) = \left(\frac{\text{rem}(439,391)}{391}\right) = -\left(\frac{48}{391}\right)\\
&= -\left(\frac{4^2}{391}\right)\left(\frac{3}{391}\right) = -\left(\frac{3}{391}\right) = -(-1)^{(391-1)(3-1)/4}\left(\frac{391}{3}\right)\\
&= \left(\frac{1}{3}\right) = 1
\end{aligned}$$

EJERCICIOS

6.1 Calcule los residuos cuadráticos módulo 9.

6.2 Muestre que si p es primo impar, $\displaystyle\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$

6.3 Use el símbolo de Jacobi para verificar si 48 no es residuo cuadrático módulo 391.

6.4 Use el símbolo de Legendre para verificar que si q es el más pequeño residuo *no* cuadrático módulo p (primo impar), entonces q debe ser primo.

6.5 Muestre que $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4$.

6.6 Sea p es primo impar. Muestre que $p-1$ es residuo cuadrático módulo p, si y solo si $p \equiv 1 \pmod 4$. **Ayuda:** Verifique que si $x^2 \equiv p-1 \pmod p$, entonces $x^2 \equiv -1 \pmod p$.

6.7 Sea p es primo impar y $\left(\frac{a}{p}\right) = 1$. Muestre que $p-a$ es residuo cuadrático módulo p, si y solo si $p \equiv 1 \pmod 4$.

6.8 Muestre que $\left(\frac{a}{5}\right) = 1$ si $a \equiv \pm 1 \pmod 5$, y $\left(\frac{a}{5}\right) = -1$ si $a \equiv \pm 2 \pmod 5$. **Ayuda:** reciprocidad cuadrática y reducción módulo 5.

6.9 Sea $n > 1$. Muestre que si p es factor primo de n^2+1, entonces $p \equiv 1 \pmod 4$.

6.10 Sea p es primo impar y $\left(\frac{a}{p}\right) = 1$. Muestre que $p-a$ es no es residuo cuadrático módulo p, si y solo si $p \equiv 3 \pmod 4$.

6.11 Sea p primo impar. Muestre que si $\left(\frac{a}{p}\right) = 1$, entonces el inverso de a es residuo cuadrático módulo p.

6.12 Sea p primo y $p \nmid A$. Si $Ax^2+Bx+C \equiv 0 \pmod p$, muestre que $(2Ax+B)^2 \equiv B^2 - 4AC \pmod p$ **Ayuda:** En $Ax^2+Bx+C \equiv 0 \pmod p$ multiplique por $4A$ y agrupe.

6.13 Resolver la congruencia $3x^2 - 4x + 7 \equiv 0 \pmod{13}$

6.14 Muestre que $3x^2 + 7x + 5 \equiv 0 \pmod{13}$ no tiene solución.

6.15 Si p es primo impar, probar que $\frac{p-1}{2} - \left[\!\left[\frac{p}{4}\right]\!\right] \equiv \frac{p^2-1}{8} \pmod 2$ para los casos $p = 8k+1$, $p = 8k-3$.

6.16 Sea p primo impar, $\operatorname{mcd}(a,p)=1$ y b raíz primitiva módulo p. Sea $a \equiv b^s \pmod{p}$. Muestre que si s es par, entonces a es residuo cuadrático; sino, a no es residuo cuadrático.

6.17 Usar el criterio de Euler para determinar si $a=54$ es residuo cuadrático módulo $p=97$.

6.18 ¿Qué puede decir de $\left(\frac{a}{2}\right)$?

6.19 ¿Es 2 residuo cuadrático módulo 3181?

6.20 Sean $p>q$ ambos primos impares. Muestre que $\left[\!\left[\frac{q}{p}\frac{p-1}{2}\right]\!\right]=\frac{q-1}{2}$. **Ayuda:** Muestre que $\frac{q-1}{2}\leq\frac{q}{p}\frac{p-1}{2}<\frac{q-1}{2}+1$.

6.21 ¿Es 3797 residuo cuadrático módulo 7297?

6.22 ¿ $\left(\frac{-1}{17}\right)=-\left(\frac{1}{17}\right)$?

6.23 Sea p primo >3. Muestre que si $p\equiv 3 \pmod 4$, entonces $\left(\frac{3}{p}\right)=-1$ si $p\equiv 2 \pmod 3$. **Ayuda:** Ley de Reciprocidad Cuadrática.

6.24 Sea p primo impar. $\left(\frac{3}{p}\right)=1$ si y solo si $p\equiv 1 \pmod{12}$.

6.25 Sea p primo impar. Muestre que la congruencia $x^2+3\equiv 0 \pmod p$ tiene solución si y solo si p es un primo de la forma $3h+1$.

6.26 Probar que $x^{(p-1)/2}\equiv 1 \pmod p$ tiene $(p-1)/2$ soluciones módulo p.

6.27 Sea $p_1,...,p_s$ primos de la forma $8k+7$ y sea $N=(4p_1p_2\cdots p_s)^2-2$.

a) Probar, usando residuos cuadráticos, que los divisores primos impares de N tienen la forma $8k+1$ o $8k+7$.

b) Probar que no todos los divisores primos impares de N tienen la forma $8k+1$

c) Probar que hay infinitos primos de la forma $8k+7$.





ESTIMACIONES, ESTADÍSTICAS Y PROMEDIOS

El propósito de este capítulo es estudiar comportamiento "típico" de algunas funciones aritméticas para tomar decisiones a la hora de crear heurísticas para resolver algún problema. Por ejemplo, nos interesa tener estimaciones para poder responder preguntas tales como: ¿La mayoría de los números tienen factores primos pequeños?, ¿Los números altamente compuestos son escasos?, ¿Cuál es el tamaño típico del factor más grande de un número?, etc.

7.1 Funciones Aritméticas

La función aritmética $\tau(n)$ cuenta cuántos divisores positivos, primos y compuestos, tiene n. Por ejemplo, los divisores de 8 son 1,2,4; así $\tau(8) = 4$. La función $\sigma(n)$ es definida como la suma de los divisores, tanto primos como compuestos, de n. Por ejemplo, $\sigma(8) = 1 + 2 + 4 = 7$. Formalmente,

$$\tau(n) = \sum_{d|n} 1 \quad \text{y} \quad \sigma(n) = \sum_{d|n} d$$

Sea $s(n) = \sigma(n) - n$, es decir, $s(n)$ es la suma de divisores *propios* de n (a veces se usa el arcaísmo "parte alícuota" en vez de divisor propio). Decimos que un entero n es *deficiente* si $s(n) > n$, es *abundante* si $s(n) > n$ y que es *perfecto* si $s(n) = n$. Por ejemplo, $s(8) = 7 < 8$, así que 8 es deficiente. $s(12) = 16$, así 12 es abundante. Los divisores de 6 son 1,2,3 y 6, por tanto $s(6) = 1 + 2 + 3 + 6 \ - \ 6 \ = \ 6$, por tanto 6 es perfecto.

τ y σ se calculan fácil si n es potencia de un primo.

Lema 7.1

Sea p primo y $n = p^k$, , entonces $\tau(n) = k + 1$ y $\sigma(n) = \dfrac{p^{k+1} - 1}{p - 1}$.

Prueba: Los divisores de d de p^k son $1, p, p^2, ..., p^k$. Hay $k + 1$ divisores. La suma es

$$1 + p + p^2 + ... + p^k = \frac{1 - p^{k+1}}{1 - p} = \frac{p^{k+1} - 1}{p - 1}$$

En el siguiente lema se muestra que τ y σ son multiplicativas, esto nos permite calcular τ y σ si conocemos la descomposición prima de n.

Lema 7.2

Si $\text{mcd}(m,n) = 1$, entonces $\tau(nm) = \tau(n)\tau(m)$ y $\sigma(nm) = \sigma(n)\sigma(m)$

Prueba: La a idea la podemos ver con un ejemplo: Sea $n = 9$ y $n = 4$, ambos son primos relativos. Ahora, hacemos un arreglo rectangular como el que está a la izquierda de la tabla (7.1). Las únicas filas en consideración son las filas que inician con un divisor de 9. Luego, solo marcamos las entradas[5] $d_i \cdot d_j$ si $d_i|9$ y $d_j|4$. Simplificando, lo que nos queda es un arreglo rectangular $\tau(9)\tau(4)$.

	1	2	3	4
1	$1\cdot 1$	$1\cdot 2$		$1\cdot 4$
2				
3	$3\cdot 1$	$3\cdot 2$		$3\cdot 4$
4				
5				
6				
7				
8				
9	$9\cdot 1$	$9\cdot 2$		$9\cdot 4$

$\longrightarrow$

	1	2	4
1	$1\cdot 1$	$1\cdot 2$	$1\cdot 4$
3	$3\cdot 1$	$3\cdot 2$	$3\cdot 4$
9	$9\cdot 1$	$9\cdot 2$	$9\cdot 4$

Tabla 7.1. Si $\text{mcd}(9,4) = 1$, entonces $\tau(9\cdot 4) = \tau(9)\tau(4)$

La prueba para $\sigma(nm)$ es una modificación de la prueba de $\tau(m)\tau(n)$. Solo necesitamos notar que $\sigma(nm)$ es la suma de todas las entradas de la tabla simplificada.
La prueba formal queda como ejercicio.

Teorema 7.1

Si la factorización prima de n es $p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$, entonces

$$\tau(n) = (k_1+1)(k_2+2)\cdots(k_s+1) \quad \text{y} \quad \sigma(n) = \prod_{i=1}^{s} \frac{p_i^{k_i}-1}{p_i-1}$$

Prueba: Como $p_1^{k_1}, p_2^{k_2}, \cdots, p_s^{k_s}$ son primos relativos dos a dos, entonces

$$\tau(n) = \tau\left(p_1^{k_1}\right) \cdot \tau\left(p_2^{k_2}\right) \cdots \tau\left(p_s^{k_s}\right) = (k_1+1)(k_2+2)\cdots(k_s+1)$$

y similarmente para $\sigma(n)$

σ y τ son ejemplos de funciones definidas sobre los números naturales. En vez de considerar este tipo de funciones como objetos aislados, es de mucha ayuda verlas como objetos más generales y estudiar la relación entre ellas por medio de una operación "$*$" (llamada convolución).

[5] Recordemos que si $\text{mcd}(m,n) = 1$ y si $d|mn$, entonces $d = ab$ con $a|m$ y $b|n$.

Una función f definida sobre los números naturales, se llama función aritmética. Por ejemplo,

$$\begin{aligned} u(n) &= 1 \text{ para todo n,} \\ N(n) &= n \text{ para todo n,} \\ e(n) &= \begin{cases} 1 & \text{si } n=1 \\ 0 & \text{si } n>1 \end{cases} \end{aligned}$$

Definición 7.1 (Convolución).

Sean f y g funciones aritméticas. La convolución de f y g, se denotada $f*g$, es una función aritmética definida por

$$f*g(n) = \sum_{d|n} f(d)g(n/d)$$

Como los divisores de n ocurren en pares (es decir, si $d|n \implies n = dk$ y entonces $(n/d)|n$), podemos escribir

$$f*g(n) = \sum_{\substack{c,d \\ n=cd}} f(d)g(c)$$

Ejemplo 7.1

Calcule $N*u$

Solución: $N*u(n) = \sum_{\substack{c,d \\ n=cd}} N(d)u(c) = \sum_{d|n} d\cdot 1 = \sigma(n)$

Ejemplo 7.2

Calcule $u*u$

Solución: $u*u(n) = \sum_{\substack{c,d \\ n=cd}} u(d)u(c) = \sum_{d|n} 1 = \tau(n)$

Teorema 7.2

Sean f,g y h funciones aritméticas, entonces

a.) $f*g = g*f$

b.) $(f*g)*h = f*(g*h)$

c.) $f*e = f$ para cualquier función aritmética f

Prueba: Ejercicio.

La función μ de Möbius se define así:

- $\mu(1) = 1$,
- si $n > 1$ tiene factorización prima $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$, entonces

$$\mu(n) = \begin{cases} 0 & \text{si } k_i > 1, \text{ para algún } i = 1,2,...,s \\ (-1)^s & \text{si } k_i = 1, \text{ para todo } i = 1,2,...,s \end{cases}$$

Así, por ejemplo $\mu(2 \cdot 3 \cdot 13) = (-1)^3 = -1$ mientras que $\mu(2 \cdot 3^2 \cdot 13) = 0$.

La función de Möbius es importante porque $f = g * u \Leftrightarrow g = f * \mu$. Esta es una fórmula muy útil y se le llama *fórmula de inversión* de Möbius.

Lema 7.3

$\mu * u = e$, es decir, $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1. \end{cases}$

Prueba: Si $n = 1$, $\sum_{d|1} \mu(d) = \mu(1) = 1$. Para probar el caso $n > 1$, empecemos con un ejemplo: Si $n = 3 \cdot 5^3 \cdot 7$, los divisores de n que contribuyen con un sumando no nulo se pueden escribir en pares, 3, $3 \cdot 7$, $3 \cdot 5$, $3 \cdot 5 \cdot 7$, 5, $5 \cdot 7$. Los divisores se dividen en dos grupos de igual cardinalidad, los que son divisibles por 7 y los que no. Si d es divisor del primer grupo, $d \cdot 7$ es divisor del segundo grupo. Observemos que $\mu(d) = -\mu(d \cdot 7)$, por tanto la suma cancela: $\sum_{d|n} \mu(d) = \mu(3) + \mu(3 \cdot 7) + ... = -1 + 1 + 1 - 1 - 1 + 1 = 0$. Formalmente,

Si $n > 1$ tiene factorización prima $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$; los únicos divisores d de n que contribuyen con un sumando no nulo, son los divisores que son productos de primos distintos. Estos divisores d se pueden dividir en dos grupos de igual tamaño; $D_1 = \{d : p_s | d\}$ y $D_2 = \{d : p_s \nmid d\}$, es decir, los productos que no tienen a p_s y estos mismos agregando p_s : $d \in D_1 \Leftrightarrow dp_s \in D_2$. Ahora, como $\mu(d) = -\mu(dp_s)$, entonces hay tantos divisores que contribuyen con -1 a la suma como divisores que contribuyen con 1, como se quería mostrar.

Teorema 7.3 (Fórmula de Inversión).

Sean f y g son funciones aritméticas,

$$\text{Si } f(n) = \sum_{d|n} g(d), \quad \text{entonces} \quad g(n) = \sum_{d|n} f(d)\mu(n/d)$$

e inversamente.

Prueba: Usando la notación de convolución, hay que probar que $f = g * u \Longleftrightarrow g = f * \mu$.

$''\Longrightarrow''$ $f = g * u \Longrightarrow f * \mu = (g * u) * \mu = g * (u * \mu) = g * (\mu * u) = g * e = g$.

" $\Longleftarrow$ " Ejercicio.

Ejemplo 7.3

Muestre que $\sum_{d|n} \sigma(d)\boldsymbol{\mu}(n/d) = n$ para toda $n \in \mathbb{Z}^+$.

Solución: Como $\sigma = N * u$, entonces por inversión de Möbius, $N = \sigma * \boldsymbol{\mu}$, que es lo que se quería.

7.2 A los números primos les gusta los juegos de azar.

La probabilidad de que un número natural, tomado al azar, sea divisible por p es $1/p$. ¿Qué significa "tomar un número natural al azar"?. Los naturales son un conjunto infinito, así que no tiene sentido decir que vamos a tomar un número al azar. Lo que si podemos es tomar un número de manera aleatoria en un conjunto finito $\{1,2,...,n\}$ y luego (atendiendo al modelo frecuentista de probabilidad) ver que pasa si n se hace grande (i.e. $n \longrightarrow \infty$).

Hagamos un pequeño experimento: Fijamos un número p y seleccionamos de manera aleatoria un número en el conjunto $\{1,2,...,n\}$ y verificamos si es divisible por p. El experimento lo repetimos m veces y calculamos la frecuencia relativa. En la tabla que sigue, hacemos este experimento varias veces para n, m y p.

n	m	p	Frecuencia relativa
100000	10000	5	0.1944
			0.2083
			0.2053
			0.1993
10000000	100000	5	0.20093
			0.19946
			0.1997
			0.20089
100000000	1000000	5	0.199574
			0.199647

Tabla 7.2. Resultado del experimento.

Y efectivamente, parece que "la probabilidad" de que un número tomado al azar en el conjunto $\{1,2,...,n\}$ sea divisible por $p = 5$ es $1/5 = 0.2$

De una manera sintética: Sea $E_p(n) =$ los múltiplos de p en el conjunto $\{1,2,...,n\}$. Podemos calcular la proporción de estos múltiplos en este conjunto, es decir, podemos calcular $\dfrac{E_p(n)}{n}$

para varios valores de n

n	Múltiplos de $p=5$	Proporción
100	20	0.2
10230	2046	0.2
100009	20001	0.199992
1000000	199999	0.199999

Tabla 7.3

Parece que en el conjunto $\{1,2,...,n\}$, la proporción de los múltiplos de $p=5$ se aproxima a $1/5$, conforme n se hace grande. ¿Significa esto que la probabilidad de que un número natural, tomado al azar, sea divisible por 5 es $1/5$?. Por ahora, lo único que podemos decir es que este experimento sugiere que la densidad (o la proporción) de los múltiplos de 5 en $\{1,2,...,n\}$ parece ser $1/5$ conforme n se hace grande. Generalizando,

Definición 7.2

Sea E un conjunto de enteros positivos con alguna propiedad especial y sea $E(N) = E \bigcap \{1,2,...,N\}$. La densidad (o medida relativa) de E se define como

$$D[E] = \lim_{n\to\infty} \frac{E(n)}{n}$$

siempre y cuando este límite exista.

¿Es esta densidad una medida de probabilidad en el modelo axiomático?. No, porque resulta no ser aditiva, como el modelo exige (ver [10]). Aunque en el esquema frecuentista se puede ver la densidad como la "probabilidad" de que un entero positivo, escogido aleatoriamente, pertenezca a E, aquí identificamos este término con *densidad o proporción*. Tenemos,

Teorema 7.4

La densidad de los naturales divisibles por p es $\frac{1}{p}$, es decir, si E_p es el conjunto de enteros positivos divisibles por p, entonces

$$D[E_p] = \lim_{n\to\infty} \frac{E_p(n)}{n} = \frac{1}{p}$$

Prueba: Para calcular el límite necesitamos una expresión analítica para $E_p(n)$. Como existen p,r tales que $n = pk + r$ con $0 \leq r < p$, entonces $kp \leq n < (k+1)p$, es decir, hay exactamente k múltiplos positivos de p que son menores o iguales a n. Luego $E_p(n) = k = \frac{n-r}{p}$. Por lo tanto, $D[E_p] = \lim_{n\to\infty} \frac{E_p(n)}{n} = \lim_{n\to\infty} \frac{(n-r)/p}{n} = \lim_{n\to\infty} \frac{1}{p} - \frac{r}{pn} = \frac{1}{p}$

Un hecho de gran importancia es este: Si p,q son primos, ser divisible por p y por q son eventos técnicamente independientes, es decir, $D[E_p \cap E_q] = D[E_p]D[E_q]$. Una de sus consecuencias (no tan inmediata) es que los divisores primos de n se distribuyen de acuerdo a la ley normal (ver [10]).

7.3 Orden de Magnitud

Necesitamos un mecanismo flexible para comparar funciones. Esto es necesario, porque a menudo nos interesa reemplazar funciones complicadas con otras más simples. En la parte práctica, esto nos permite establecer términos de error en una estimación, de una manera más flexible.
Para comparar dos funciones f y g, es conveniente primero definir la relación "$\ll$" (se lee "dominada por"): Decimos que

$$f(x) \ll g(x) \quad \text{conforme} \quad x \to \infty$$

si podemos encontrar una constante C y x_0 tal que

$$f(x) \leq Cg(x) \quad \text{cuando} \quad x > x_0$$

Para establecer esta desigualdad, a menudo es muy útil usar el hecho de que si f es creciente, entonces $a \leq b$ cuando $f(a) \leq f(b)$. A veces se puede usar la derivada para establecer que f es creciente (o decreciente) en un intervalo.

Ejemplo 7.4

Muestre que $3x^3 - x^2 + 1 \ll x^3$ conforme $x \to \infty$

Solución: Tenemos que encontrar C y x_0 tal que $x^3 - x^2 + 1 \leq Cx^3$ cuando $x \geq x_0$.

Como $1 - x^2 < 0$ si $x > 1$, entonces $3x^3 - x^2 + 1 < 3x^3$ si $x > 1$. Por tanto basta tomar $C = 3$ y $x_0 = 1$ para que se cumpla la definición.

Ejemplo 7.5

Muestre que $\exp(\sqrt{\log(x)}) \ll x$ conforme $x \to \infty$

Solución: $\exp(x)$ y $\log(x)$ son funciones crecientes, entonces

$$\begin{array}{rcll} \exp(\sqrt{\log(x)}) & \leq & x & \iff \text{(tomando logaritmos)} \\ \sqrt{\log(x)} & \leq & \log(x) & \iff \text{(cuadrados a ambos lados)} \\ \log(x) & \leq & \log^2(x), & (*) \end{array}$$

ahora, como $u \leq u^2$ si $u \geq 1$, la desigualdad $(*)$ se cumple si $x > e$. Por tanto, basta tomar $C = 1$, y $x_0 = e$ para que se cumpla la definición.

O grande de Landau. En general, nos interesa una manera de decir que f y g son funciones parecidas en orden excepto por un término de error *dominado* por una función h. Decimos que

$$f(x) = g(x) + O(h(x)) \quad \text{si} \quad |f(x) - g(x)| \ll h(x)$$

En particular, si $g(x) \equiv 0$,

$$f(x) = O(h(x)) \quad \text{si} \quad f(x) \ll h(x)$$

Ejemplo 7.6

Observe que $f(x) = O(1)$ significa que f es una función acotada en un intervalo $]x_0, \infty[$. También, usando los dos ejemplos anteriores, $3x^3 - x^2 + 1 = O(3x^3)$ y $\exp(\sqrt{\log(x)}) = O(x)$.

Ejemplo 7.7

Muestre que $\dfrac{x}{x+1} = 1 + O\left(\dfrac{1}{x}\right)$.

Solución: $|x/(x+1) - 1| = 1/(x+1) < 1/x$ si $x > 0$. Así, tomando $C = 1$ y $x_0 = 0$, el término de error es $O(1/x)$.

Ejemplo 7.8

Sean n, d enteros positivos, Muestre que $[\![n/d]\!] = n/d + O(1)$.

Solución: Por el algoritmo de la división, existe $k, r \in \mathbb{Z}$ tal que $n = k \cdot d + r$ con $0 \leq r < d$ o también $n/d = k + r/d$. Luego, $[\![n/d]\!] = k = (n-r)/d$. Ahora, $|[\![n/d]\!] - n/d| = r/d < 1$ para cada $n \geq 0$. Así, tenemos $[\![n/d]\!] = n/d + O(1)$, tomando $C = 1$.

o pequeña. La definición de O grande requiere la existencia de una constante C tal que $f \leq Cg$. La definición de la o pequeña es similar, solo que esta vez pedimos que $0 \leq f \leq Cg$ para *toda* $C > 0$. En lo que sigue, solo hacemos referencia un par de veces a este concepto, así que solo vamos a dar la definición.

Definición 7.3

Sea f, g funciones. Decimos que $f = o(g)$ si para toda $c \in \mathbb{R}^+$, existe x_c tal que $0 \leq f(x) \leq c \cdot g(x)$ si $x > x_c$.

7.4 Teorema de los números primos

Ya sabemos que los primos son infinitos. De aquí en adelante hay una pregunta muy natural: ¿cuántos primos hay entre 2 y x?. Por ejemplo, 2,3,5,7 son los primos inferiores a $x = 10$, así que hay 4 primos entre 2 y 10.

La función que se usa para contar los primos por debajo de x se denota con $\pi(x)$: Por ejemplo, $\pi(2) = 1$, $\pi(10) = 4$ y $\pi(\sqrt{1000}) = 11$.

Para la función $\pi(x)$ no hay una fórmula sencilla. Algunas fórmulas actuales son variaciones un poco más eficientes que la fórmula recursiva de Legendre (1808).

7.4.1 Fórmula de Legendre para $\pi(x)$.

Esta fórmula esta basada en el principio de Inclusión-Exclusión. Básicamente dice que el conjunto $\{1,2,...,[\![x]\!]\}$ es la unión del entero 1, los primos $\leq x$ y los enteros compuestos $\leq x$,

$$[\![x]\!] = 1 + \pi(x) + \#\{\text{ enteros compuestos} \leq x\}$$

Un entero compuesto en el conjunto $A = \{1,2,...,[\![x]\!]\}$ tiene al menos un divisor primo menor o igual a $\sqrt{x}$. Esto nos ayuda a detectar los números compuestos en A : Solo tenemos que contar los elementos de A con un divisor primo $\leq \sqrt{x}$.

Los números divisibles por p e inferiores a x son los k números $p < 2p < ... < k \cdot p \leq x$. Como $kp \leq x < (k+1)p$, entonces $k = [\![x/p]\!]$. Así, $[\![x/p]\!]$ cuenta la cantidad de enteros $\leq x$ divisibles por p.

Ahora, ¿$\#\{$ enteros compuestos $\leq x\}$ es igual a al conteo total de los múltiplos de cada primo $p_i \leq \sqrt{x}$? No, pues este conteo incluye a los propios primos p_i, así que hay que reponer con $\pi(\sqrt{x})$ para hacer una corrección. Pero también habría que restar los compuestos que son divisibles por p_i y p_j pues fueron contados dos veces, pero esto haría que los números divisibles por p_i, p_j, p_k fueran descontados una vez más de lo necesario así que hay que agregar una corrección para estos números, y así sucesivamente.

Ejemplo 7.9

Si $x = 30$, los primos menores que $[\![\sqrt{30}]\!] = 5$ son 2,3 y 5.

$[\![30/2]\!] = 15$ cuenta $\{2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\}$
$[\![30/3]\!] = 10$ cuenta $\{3,6,9,12,15,18,21,24,27,30\}$
$[\![30/5]\!] = 6$ cuenta $\{5,10,15,20,25,30\}$

En el conteo $[\![30/2]\!] + [\![30/3]\!] + [\![30/5]\!]$:

- se contaron los primos 2,3 y 5.

- $6,12,18,24,30$ fueron contados dos veces como múltiplos de $2,\ 3$
- $10,20,30$ fueron contados dos veces como múltiplos de $2,\ 5$
- $15,30$ fueron contados dos veces como múltiplos de $3,\ 5$
- 30 fue contado tres veces como múltiplo de $2,3$ y 5.

Ejemplo 7.0 (continuación).

Finalmente,

$$\begin{aligned} \#\{\text{ enteros compuestos} \leq 30\} &= [\![30/2]\!] + [\![30/3]\!] + [\![30/5]\!] \\ &- [\![30/(2\cdot 3)]\!] - [\![30/(2\cdot 5)]\!] - [\![30/(3\cdot 5)]\!] \\ &+ [\![30/(2\cdot 3\cdot 5)]\!] \\ &= 31 - 3 - 5 - 3 - 2 + 1 = 19 \end{aligned}$$

El último sumando se agrega pues el 30 fue contado tres veces pero también se resto tres veces.

Observe ahora que en $\{1,2,...,30\}$ hay 19 compuestos y el 1, así que quedan 10 primos.

Fórmula de Legendre para $\pi(x)$.

Sea p_i el $i-$ésimo primo. La fórmula de Legendre es,

$$1+\pi(x) = \pi(\sqrt{x}) + [\![x]\!] - \sum_{p_i\leq\sqrt{x}} \left[\frac{x}{p_i}\right] + \sum_{p_i<p_j\leq\sqrt{x}} \left[\frac{x}{p_ip_j}\right] - \sum_{p_i<p_j<p_k\leq\sqrt{x}} \left[\frac{x}{p_ip_jp_k}\right] + \cdots$$

Para efectos de implementación es mejor poner $\alpha = \pi(\sqrt{x})$ y entonces la fórmula queda

$$1+\pi(x) = \pi(\sqrt{x}) + [\![x]\!] - \sum_{i\leq\alpha} \left[\frac{x}{p_i}\right] + \sum_{i<j\leq\alpha} \left[\frac{x}{p_ip_j}\right] - \sum_{i<j<k\leq\alpha} \left[\frac{x}{p_ip_jp_k}\right] + \cdots$$

Ejemplo 7.10

Calcular $\pi(100)$

Solución: Como $\sqrt{100} = 10$, solo usamos los primos $\{2,3,5,7\}$.

$$\begin{aligned}
1+\pi(100) &= \pi(10)+\llbracket 100\rrbracket \\
&\quad -(\llbracket 100/2\rrbracket+\llbracket 100/3\rrbracket+\llbracket 100/5\rrbracket+\llbracket 100/7\rrbracket) \\
&\quad +\llbracket 100/2\cdot 3\rrbracket+\llbracket 100/2\cdot 5\rrbracket+\llbracket 100/2\cdot 7\rrbracket+\llbracket 100/3\cdot 5\rrbracket+\llbracket 100/3\cdot 7\rrbracket+\llbracket 100/5\cdot 7\rrbracket \\
&\quad -(\llbracket 100/2\cdot 3\cdot 5\rrbracket+\llbracket 100/2\cdot 3\cdot 7\rrbracket+\llbracket 100/2\cdot 5\cdot 7\rrbracket+\llbracket 100/3\cdot 5\cdot 7\rrbracket) \\
&\quad +\llbracket 100/2\cdot 3\cdot 5\cdot 7\rrbracket \\
&= 4+100-(50+33+20+14)+(16+10+7+6+4+2)-(3+2+0+1)+0 \;=\; 26
\end{aligned}$$

El problema con esta fórmula es la cantidad de cálculos que se necesita para calcular las correcciones.

Las cantidad de partes enteras $\llbracket x/(p_{i_1}p_{i_2}\cdots p_{i_k})\rrbracket$ corresponde a la cantidad de subconjuntos no vacíos $\{i_1,i_2,\cdots,i_k\}$ de $\{1,2,...,\alpha\}$, es decir, hay que calcular $2^\alpha-1$ partes enteras.

Si quisieramos calcular $\pi(10^{33})$, entonces, puesto que $\sqrt{10^{33}}=10^{18}$, tendríamos que tener los primos $\leq 10^{18}$ y calcular las partes enteras $\left[x/(p_{k_1}p_{k_2}...p_{k_j})\right]$ que corresponden al cálculo de todos los subconjuntos de $\{1,2,...,\pi(10^{18})\}$. Como $\pi(10^{18})=24739954287740860$, tendríamos que calcular

$$2^{24739954287740860}-1 \;\; \text{partes enteras.}$$

que constituye un número nada razonable de cálculos.

7.4.2 Fórmula de Meisel para $\pi(x)$.

La fórmula de Meisel es un re-arreglo de la fórmula de Legendre. Pongamos

$$\text{Legendre}(x,\alpha)=\sum_{i\leq\alpha}\left[\frac{x}{p_i}\right]-\sum_{i<j\leq\alpha}\left[\frac{x}{p_ip_j}\right]+\sum_{i<j<k\leq\alpha}\left[\frac{x}{p_ip_jp_k}\right]+\cdots$$

Así $\pi(x)=\llbracket x\rrbracket-1+\alpha-\text{Legendre}(x,\alpha)$ donde $\alpha=\pi(\sqrt{x})$, es decir, $\text{Legendre}(x,\alpha)-\alpha$ cuenta la cantidad de números compuestos $\leq x$ o, en otras palabras, los números $\leq x$ con al menos un divisor primo inferior a $\alpha=\sqrt{x}$.

Ahora $\text{Legendre}(x,\alpha)$ va a tener un significado más amplio: Si $\alpha\in\mathbb{N}$,

$$\text{Legendre}(x,\alpha)=\sum_{i\leq\alpha}\left[\frac{x}{p_i}\right]-\sum_{i<j\leq\alpha}\left[\frac{x}{p_ip_j}\right]+\sum_{i<j<k\leq\alpha}\left[\frac{x}{p_ip_jp_k}\right]+\cdots$$

es decir, $\text{Legendre}(x,\alpha)-\alpha$ cuenta los compuestos $\leq x$ que son divisibles por primos $\leq p_\alpha$. La resta es necesaria pues la manera de contar cuenta también los primos $p_1,\ p_2,\ ...,p_\alpha$

Ahora, dividamos los enteros en cuatro grupos: $\{1\}$, $\{\text{primos }\leq x\}$, $C_3\cup C_4=$ los compuestos $\leq x$.

$\llbracket x\rrbracket=1+\pi(x)+\#C_3+\#C_4$

$\#C_3$: Es la cantidad de números compuestos $\leq x$ con al menos un divisor primo $\leq p_\alpha$, es decir Legendre$(x,\alpha)-\alpha$.

$\#C_4$: son los compuestos $\leq x$ cuyos divisores primos son $> p_\alpha$: Aquí es donde entra en juego la escogencia de α para determinar la cantidad de factores primos de estos números.

Sea p_i el $i-$ésimo primo. Sean p_α y p_β tal que $p_\alpha^3 \leq x < p_{\alpha+1}^3$ y $p_\beta^2 \leq x < p_{\beta+1}^2$. En otras palabras: $\alpha = \pi(\sqrt[3]{x})$ y $\beta = \pi(\sqrt{x})$.

Consideremos la descomposición prima de $n \in C_4$, $n = p_{i_1} \cdot p_{i_2} \cdots p_{i_k}$ con $\alpha < p_{i_1} < p_{i_2} < ... < p_{i_k}$ y $k \geq 2$. Como $p_{\alpha+1}^k \leq p_{i_1} \cdot p_{i_2} \cdots p_{i_k} \leq x < p_{\alpha+1}^3 \implies k = 2$.

Así que estos números en C_4 son de la forma $p_{\alpha+k}p_j \leq x$, $a+k \leq j$, $k = 1,2,...$
Pero la cantidad de números $p_{\alpha+k}p_j$ es igual a la cantidad de p_j's tal que $p_j \leq x/p_{\alpha+k}$: $\pi(x/p_{\alpha+k}) - (\alpha+k)$.

Además $\alpha < \alpha+k \leq \beta$ pues si $\alpha+k = \beta$, $p_\beta \cdot p_\beta = p_\beta^2 \leq x$ pero $p_{\beta+1}p_j \geq p_{\beta+1}^2 > x$.

Así, usando la fórmula $\sum_{i=1}^{n-1} i = n(n-1)/2$,

$$\#C_4 = \sum_{\alpha<i\leq\beta} \{\pi(x/p_i) - (i-1)\} = \frac{1}{2}\beta(\beta-1) - \frac{1}{2}\alpha(\alpha-1) + \sum_{\alpha<i\leq\beta} \pi(x/p_i)$$

¿Cuál es la ganancia? Mientras que con la fórmula de Legendre necesitamos conocer $\pi(\sqrt{x})$ y calcular con primos $\leq \sqrt{x}$, con la fórmula de Meisel solo necesitamos conocer hasta $\pi(\sqrt[3]{x})$ y calcular con primos $\leq \sqrt[3]{x} < \sqrt{x}$.

Ejemplo 7.11

Calcule $\pi(100)$ usando la fórmula de Meisel.

Solución: Como $\alpha = \pi(\sqrt[3]{100}) = 2$ y $\beta = \pi(\sqrt{100}) = 4$, solo vamos a usar los primos $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$.

$$\begin{aligned} \text{Legendre}(100,2) &= [\![100/2]\!] + [\![100/3]\!] + [\![100/2\cdot 3]\!] \\ &= 50 + 33 - 16 = 67 \end{aligned}$$

$$\begin{aligned} \text{Meisel}(100,2,4) &= \pi(100/5) + \pi(100/7) \\ &= \pi(20) + \pi(4) = 8 + 6 = 14 \end{aligned}$$

Así, $\pi(100) = 100 + 6 - 0 - 67 - 14 = 25$

Mathematica (Wolfram Research Inc.) implementa $\pi(x)$ con el comando PrimePi$[x]$ hasta $x \approx 8 \times 10^{13}$. En esta implementación, si x es pequeño, se calcula $\pi(x)$ usando colado y si x es grande se usa el algoritmo Lagarias-Miller-Odlyzko.

7.5 Estimación de $\pi(x)$. Teorema de los números primos.

El cálculo de $\pi(x)$ de manera directa es bastante complicado y requiere mucho esfuerzo computacional. En general, no podemos responder de manera exacta todo el tiempo. Curiosamente, hay fórmulas relativamente simples para responder con una aproximación del valor de $\pi(x)$ para valores grandes de x. Legendre y Gauss iniciaron el estudio de esta estimación contando primos en intervalos de longitud adecuada y calculando proporciones, en busca de un ley que gobernara esta distribución.

La frecuencia relativa $\pi(n)/n$ calcula la proporción de primos en el conjunto $A = \{1,2,...,n\}$. Aunque la distribución de los primos entre los enteros parece irregular, el comportamiento promedio si parece ser agradable. Como dijimos antes, basándose en un estudio empírico de tablas de números primos, Legendre y Gauss (en 1792, a la edad de 15 años) conjeturan que la ley que gobierna el cociente $\pi(n)/n$ es aproximadamente igual a $\dfrac{1}{\ln(n)}$.

En [9] se indica que Gauss y Legendre llegaron a este resultado, de manera independiente, estudiando la densidad de primos en intervalos que difieren en potencias de diez: Notaron que la proporción de primos en intervalos centrados en $x = 10^n$ decrece lentamente y disminuye aproximadamente a la mitad cada vez que pasamos de x a x^2. Este fenómeno es muy bien modelado por $1/\ln(x)$ pues $1/\ln(x^2) = 0.5/\ln(x)$.

n	$\pi(n)$	$\pi(n)/n$	$1/\ln(n)$
10^7	664579	0.0664579	0.0620420
10^{11}	4118054813	0.0411805	0.0394813
10^{12}	37607912018	0.0376079	0.0361912

Tabla 7.4

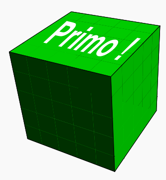
Acerca de este descubrimiento, Gauss escribió a uno de sus ex-alumnos, Johann Franz Encke, en 1849

> *"Cuando era un muchacho considere el problema de cuántos primos había hasta un punto dado. Lo que encontré fue que la densidad de primos alrededor de x es aproximadamente $1/\ln(x)$."*

La manera de interpretar esto es que si n es un número "cercano" a x, entonces es primo con "probabilidad" $1/\ln(x)$. Claro, un número dado es o no es primo, pero esta manera de ver las cosas ayuda a entender de manera muy intuitiva muchas cosas acerca de los primos.

Ejemplo 7.12

pto Como $[\![\ln(1000)]\!] = 7$, podemos usar un dado de 6 caras para decidir si un número n cercano a 1000, es (probablemente) primo



- Para decidir con un dado si un número n cercano a 10 000 es probablemente primo, debemos contruir un dado de 8 lados pues $[\![\ln(10\,000)]\!] = 9$.



Lo que afirma Gauss es lo siguiente: Si Δx es "pequeño" comparado con x (en el mundillo asintótico esto quiere decir que $\Delta x/x \to 0$ conforme $x \to \infty$) entonces

$$\frac{\pi(x+\Delta x) - \pi(x)}{\Delta x} \approx \frac{1}{\ln(x)}$$

$(\pi(x+\Delta x) - \pi(x))/\Delta x$ es la densidad de primos en le intervalo $[x,\, x+\Delta x]$ y $1/\ln(x)$ es el promedio estimado en este intervalo. Por esto decimos: $1/\ln(x)$ es la "probabilidad" de que un número n, en las cercanías de x, sea primo. Para hacer un experimento, podemos tomar $\Delta x = \sqrt{x}$ (que claramente es dominada por x),

x	$\pi(x+\Delta x) - \pi(x)$	$\frac{\pi(x+\Delta x) - \pi(x)}{\Delta x}$	$\frac{1}{\ln(x)}$
10	2	0.632	0.434
100	4	0.4	0.217
1000	5	0.158	0.144
10000	11	0.11	0.108
100000000000	12491	0.0395	0.039
1000000000000	36249	0.0362	0.036

Tabla 7.5. Densidad de primos en le intervalo $[x,\, x+\Delta x]$ con $\Delta x = \sqrt{x}$

Hadamard y de la Vallée Poussin probaron en 1896, usando métodos basados en análisis complejo, el

Teorema 7.5 (Teorema de los Números Primos).

Sea $\operatorname{Li}(x) = \int_2^x \frac{dt}{\ln(t)}$. Entonces $\pi(x) \sim \operatorname{Li}(x)$, es decir $\lim_{x\to\infty} \frac{\pi(x)}{\operatorname{Li}(x)} = 1$

La conjetura de Legendre era $\pi(x) \sim x/\ln(x)$. Esta expresión se usa mucho cuando se hacen estimaciones "gruesas":

Teorema 7.6

$\operatorname{Li}(x) \sim x/\ln(x)$, es decir $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$

7.5.1 La función Zeta de Riemann

Este tema está en el ámbito de la teoría analítica de números. Aquí solo podemos hacer una excursión algo descriptiva con solo algunos cálculos concretos que involucran a la función "zeta" de Riemann. Los resultados que se mencionan aquí fueron tomados de [9] y [2].

La aproximación a $\pi(x)$ dada por Gauss y Legendre fue encontrada por métodos empíricos. Riemann fue el primero en deducir de manera sistemática relaciones entre los números primos y las funciones matemáticas conocidas. El punto de partida de Riemann fue la relación descubierta por Euler

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}} \tag{7.1}$$

donde el producto es tomado sobre todos los primos.

Para entender esta fórmula debemos aplicar series geométricas,

$$\frac{1}{1-p^{-s}} = 1 + p^{-s} + (p^{-s})^2 + ...$$

Así,

$$\begin{aligned}\prod_{p \text{ primo}} \frac{1}{1-p^{-s}} &= (1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + ...)\\ &\cdot(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + ...)\\ &\cdot(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + ...)\\ &\cdots\end{aligned}$$

Ejemplo 7.13

Veamos un ejemplo concreto. Si $s = 1$ entonces

$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p \text{ primo}} \frac{1}{1-p^{-1}} = (1 + \frac{1}{2} + \frac{1}{2^2} + ...) \cdot (1 + \frac{1}{3} + \frac{1}{3^2} + ...) \cdot (1 + \frac{1}{5} + \frac{1}{5^2} + ...) \cdot (1 + \frac{1}{7} + \frac{1}{7^2} + ...) \cdots$$

Así, el sumando $\frac{1}{450}$ se obtiene como $\frac{1}{2 \cdot 3^2 \cdot 5^2} = \frac{1}{2} \cdot \frac{1}{3^2} \cdot \frac{1}{5^2} \cdot 1 \cdot 1 \cdots$.

El producto de los dos primeros factores sería,

$$\begin{aligned}(1 + p_1^{-1} + p_1^{-2} + ...)(1 + p_2^{-1} + p_2^{-2} + ...) &= 1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \frac{1}{p_2^3} + \frac{1}{p_2 p_1} + \frac{1}{p_2^2 p_1} \\ &+ \frac{1}{p_2^3 p_1} + \frac{1}{p_1} + \frac{1}{p_2 p_1^2} + \frac{1}{p_1^2} + \frac{1}{p_2 p_1^3} \\ &+ \frac{1}{p_2^2 p_1^2} + \frac{1}{p_2^3 p_1^2} + \frac{1}{p_2^2 p_1^3} + \frac{1}{p_2^3 p_1^3} + \frac{1}{p_1^3}\end{aligned}$$

Luego, $\zeta(1) = \sum \frac{1}{2^{\alpha_1} 3^{\alpha_2} \cdots p_n^{\alpha_n}}$ donde la suma cubre todas las combinaciones de exponentes $\alpha_i \geq 0$ y todos los primos p_i. El teorema fundamental de la aritmética dice que estos productos en los denominadores son todos los enteros positivos: $\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n}$.

Riemann toma esta identidad establecida por Euler y pone a trabajar la teoría de funciones analíticas (funciones diferenciables de variable compleja). Extiende la relación (7.2), la cual está restringida a $s > 1$ por razones de convergencia, a $s = \sigma + it$ con $\sigma > 0$ y $s \neq 1$ (en este caso $|\zeta(1)| = \infty$). La nueva función luce así

$$\zeta(s) = \frac{1}{1 - 2^{1-s}} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s} \tag{7.2}$$

Esta función converge para todos los $s \neq 1$ con $\sigma > 0$ si $s \neq 1$. Para calcular $\zeta(s)$ se usa la fórmula de Euler-Maclaurin

$$\begin{aligned}\zeta(s) &\approx \sum_{n=1}^{N-1} n^{-s} + \frac{1}{s-1} N^{1-s} + \frac{1}{2} N^{-s} \\ &+ \frac{1}{12} N^{-s-1} - \frac{s(s+1)(s+2)}{720} N^{-s-3} + \frac{s(s+1)(s+2)(s+3)(s+4)}{30240} N^{-s-5},\end{aligned}$$

Por ejemplo, tomando $N = 1000$,

$\zeta(2) \approx 1.6449340668482264... \approx \pi^2/6 = 1.6449340668482262...$

$\zeta(1/2 + 37.586178 \cdot i) = -8.910197857314728 \times 10^{-8} - 2.9437792720132805 \times 10^{-7}\, i$

En realidad, $0.5 + 37.586178158825675... \cdot i$ es el sexto cero no trivial de ζ, es decir, $\zeta(1/2 + 0.5 + 37.586178158825675... \cdot i) = 0$. A este respecto, la famosa hipótesis de Riemann dice que todos los ceros no triviales de $\zeta(s)$ son de la forma $s = 1/2 + it$. La importancia de esta hipótesis se debe a que la estimación del error en varias fórmulas relacionadas con la distribución de los números primos depende del conocimiento de regiones extensas libres de ceros de la función $\zeta(s)$. En particular,

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\ln x)$$

Para obtener una fórmula para $\pi(x)$, Riemann define la función $f(x) = \pi(x) + 1/2\pi(x^{1/2}) + 1/3\pi(x^{1/3}) + ...$, con $x > 1$ y no entero. Sorprendentemente,

$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} f(x^{1/n}) \qquad (7.3)$$

En 1859 Riemann hace la conjetura

$$f(x) = \mathrm{Li}(x) - \sum_{\rho} \mathrm{Li}(x^{\rho}) - \ln 2 + \int_x^{\infty} dt/(t(t^2-1)\ln t)$$

donde la suma corre sobre todos los ceros no triviales ρ de $\zeta(s)$, contando multiplicidad. Esto fue probado por Mangoldt en 1895. Ahora, cambiando $f(x^{1/n})$ por $\mathrm{Li}(x^{1/n})$ en (7.3), Riemann obtiene

$$\mathrm{Ri}(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \mathrm{Li}(x^{1/n}) \sim \pi(x)$$

En esta fórmula, es conveniente calcular $\mathrm{Li}(x) = \mathrm{Ei}(Log(z))$ donde $\mathrm{Ei}(z) = -\int_{-z}^{\infty} e^{-t}/t\,dt$; suponiendo que tenemos una buena implementación de esta función, por ejemplo en ([24]).

La función $\mathrm{Ri}(n)$, $n \in \mathbb{Z}^+$, se puede calcular usando la serie de Gram (1893),

$$\mathrm{Ri}(n) = 1 + \sum_{k=1}^{\infty} \frac{(\log n)^k}{k! \cdot k\zeta(k+1)},$$

esta serie exhibe convergencia muy veloz; sin embargo, la aproximación a $\pi(x)$ es aceptable si $x < 10^9$.

¿Qué tan bien se puede aproximar $\pi(x)$? El teorema de los números primos indica que $\pi(x) \sim \mathrm{Li}(x)$, es decir, el error relativo

$$\left|\frac{\mathrm{Li}(x) - \pi(x)}{\mathrm{Li}(x)}\right| \longrightarrow 0 \text{ conforme } x \longrightarrow 0.$$

Efectivamente, conforme x es grande, $\mathrm{Li}(x)$ se aproxima más y más a $\pi(x)$. Si x *no es muy grande*, se puede tener un error porcentual pequeño y un error real de varios millones, que aún así, es despreciable respecto a la magnitud de $\pi(x)$. En la tabla (7.7) se hace una comparación

entre $\pi(x)$ $\text{Li}(x)$. Los valores de $\pi(x)$ se obtuvieron de tablas especiales mientras que $\text{Li}(x)$ se calculó con $Ei(x)$.

x	$\pi(x)$	$\text{Li}(x)$	$\text{Li}(x) - \pi(x)$	$\frac{\pi(x) - \text{Li}(x)}{\text{Li}(x)}$
10^{13}	346065536839	346065645810.	108 971	-3.14×10^{-7}
10^{18}	24739954287740860	24739954309690415.	21949555	8.87×10^{-7}
10^{22}	201467286689315906290	201467286691248261498.	1932355207	9.59×10^{-12}

Tabla 7.6. Comparando $\pi(x)$ con $\text{Li}(x)$

Una mejora notable se obtiene si cambiamos $\text{Li}(x)$ por $\text{Ri}(x)$,

x	$\text{Li}(x) - \pi(x)$	$\text{Ri}(x) - \pi(x)$
10^{13}	108971.	-5773
10^{18}	21949555.	-3501366
10^{22}	1932355207.	-127132665

Tabla 7.7. Comparando $\pi(x)$ con $\text{Ri}(x)$

7.5.2 Teorema de Mertens.

En este apartado vamos a aplicar algunos cálculos aproximados para establecer un resultado muy curioso: Típicamente, los números grandes tienen factores primos pequeños.

Observemos que en el conjunto $\{1,2,3,...,9\}$ solo $3,6$ y 9 son divisibles por 3. En términos de proporciones, una tercera parte. La tabla que sigue muestra las proporciones al variar n. Es ésta tabla, d_n denota la cantidad de enteros positivos $\leq n$ que son divisibles por 3.

n	$d_n/n \approx 1/3$
8680	0.333294930875576 05
76333	0.33332896650203714
554615	0.333332131298288

Tabla 7.8. Proporción de números divisibles por 3.

Como $1/p$ es la proporción *aproximada* de números, en el conjunto $\{1,2,...,n\}$, divisibles por p, $1-1/p$ sería la proporción de números en este conjunto que *no son divisibles* por p.

Aquí estamos asumiendo demasiado porque esta proporción no es exactamente $1/p$. Este número solo es una aproximación. Si "ser divisible por p" es un evento independiente de "ser divisible por q", $\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$ sería la proporción de números en el conjunto $\{1,2,...,n\}$, que *no* son divisibles por p ni por q.

En general, $\prod_{\substack{2\leq p\leq G,\\ p \text{ primo},}} \left(1-\frac{1}{p}\right)$ sería una estimación de la proporción de números en el conjunto $\{1,2,...,n\}$, que no son divisibles por ninguno de los primos menores o iguales a G. Esto si tiene utilidad práctica, como veremos más adelante.

Ejemplo 7.14

Hagamos un experimento. Sea $d_n = \#\{m \leq n : m \text{ es divisible por } 2,3,5, \text{o } 7\}$.

n	d_n	d_n/n
103790	80066	0.7714230658059543
949971	732835	0.7714288120374201
400044	308605	0.7714276429592745
117131	90359	0.7714354013881893
124679	96181	0.7714290297483939

Tabla 7.9

La proporción de números naturales $\leq n$ divisibles por $2,3,5$ es ≈ 0.7714. Así, $1-0.7714 = 0.2286$ es la proporción de números en $\{1,2,...,n\}$ que *no* son divisibles por los primos $2,3,5$ y 7.

Y efectivamente, $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 0.228571.$

Si intentamos calcular el producto para cantidades cada vez grandes de primos, rápidamente empezaremos a tener problemas con el computador. En vez de esto, podemos usar el

Teorema 7.7 (Fórmula de Mertens).

$$\prod_{\substack{2\leq p\leq x,\\ p \text{ primo}}} \left(1-\frac{1}{p}\right) = \frac{e^{-\gamma}}{\ln(x)} + O(1/\ln(x)^2)$$

γ es la constante de Euler

Para efectos prácticos consideramos la expresión

$$\prod_{\substack{2\leq p\leq x,\\ p \text{ primo}}} \left(1-\frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\ln(x)} \approx \frac{0.5615}{\ln(x)} \quad \text{si } x \longrightarrow \infty \tag{7.4}$$

Ejemplo 7.15

Veamos la fórmula en acción,

x	$\prod_{\text{primos } p \leq \sqrt{x}} (1 - 1/p)$	$\frac{2e^{-\gamma}}{\ln(x)}$
100000	0.0965	0.0975
100000000000000	0.034833774529614024	0.03483410793219253

Tabla 7.10

También, multiplicando (7.4) por 2, la fórmula

$$\prod_{\substack{3 \leq p, \\ p \text{ primo}}}^{G} \left(1 - \frac{1}{p}\right) \sim \frac{2e^{-\gamma}}{\ln(G)} \approx \frac{1.12292}{\ln(G)}$$

nos daría la proporción aproximada de números impares que no tienen un factor primo $\leq G$.

Ejemplo 7.16

En este ejemplo se muestra que los números grandes sin factores primos pequeños no son el caso típico.

G	Proporción approx de impares sin factores primos $\leq G$.
100	0.243839
1000	0.162559
10000	0.121919
100000	0.0975355
1000000	0.0812796
10000000	0.0696682
100000000	0.0609597
1000000000	0.0541864
10000000000	0.0487678

Tabla 7.11

Esta tabla nos informa que "típicamente", los números grandes tienen factores primos pequeños.

7.6 Números Armónicos

Aunque la serie armónica $\sum_{k=1}^{\infty} \frac{1}{k}$ es divergente, la función $H_n = \sum_{k=1}^{n} \frac{1}{k}$ es muy útil en teoría analítica de números.

Lema 7.4

Existe una número real γ, llamada *constante de Euler*, tal que

$$H_n = \ln(n) + \gamma + O(1/n).$$

Prueba: Hay que mostrar que $\exists C$ tal que $0 < H_n - \ln(n) - \gamma < C \cdot 1/n$ para $n > n_0$. Usando integral de Riemann,

$$\sum_{k=1}^{n-1} \frac{1}{k} = \int_1^n \frac{1}{x}\, dx + E_n \quad \text{i.e.} \quad H_{n-1} = \ln(n) + E_n$$

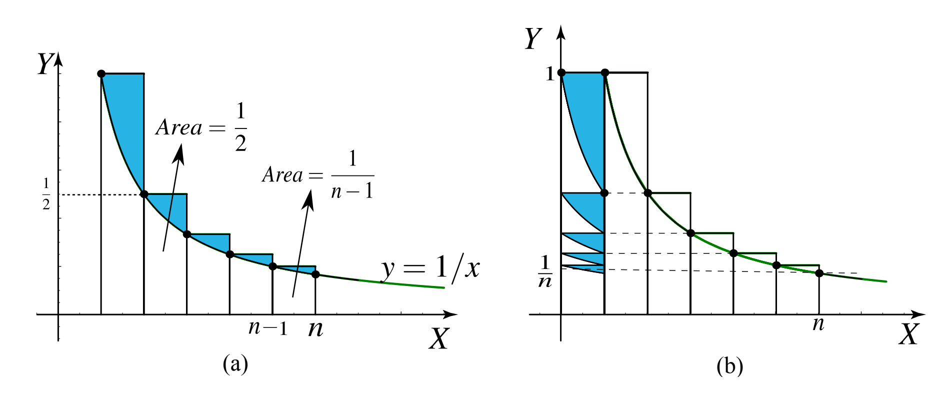


Figura 7.1. Comparando el área $\ln(n)$ con la suma H_n.

Geométricamente, H_{n-1} corresponde a la suma de las áreas de los rectángulos desde 1 hasta n y E_n la suma de las áreas de las porciones de los rectángulos sobre la curva $y = 1/x$.
En el gráfico (b) de la figura 7.1 vemos que $E_n \leq 1$ para toda $n \geq 1$, así que E_n es una función de n, que se mantiene acotada y es creciente, por lo tanto esta función tiene un límite, el cual vamos a denotar con γ. Así, $\lim_{n\to\infty} E_n = \gamma$. En particular, para cada n fijo, $\gamma > E_n$.
Como $\gamma - E_n$ corresponde a la suma (infinita) de las áreas de las regiones sombreadas en la figura 7.6, se establece la desigualdad

$$\gamma - E_n < 1/n$$

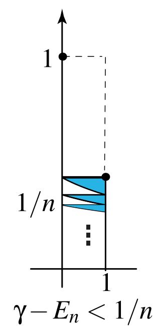
de donde

$$0 < \gamma - (H_{n-1} - \ln(n)) < 1/n.$$

Ahora restamos $1/n$ a ambos lados para hacer que aparezca H_n, tenemos

$$\frac{1}{n} > H_n - \ln(n) - \gamma > 0$$

que era lo que queríamos demostrar.



Aunque en la demostración se establece $H_n - \ln(n) - \gamma < 1/n$, la estimación del error $O(1/n)$ corresponde a una función dominada por un múltiplo de $1/n$. Veamos ahora algunos cálculos que pretender evidenciar el significado de $O(1/n)$.

n	H_n	$\ln(n)$	$\lvert H_n - \ln(n) - \gamma\rvert$	$1/n$
170000	12.62077232	12.62076938	$2.94117358 \times 10^{-6}$	$5.88235294 \times 10^{-6}$
180000	12.67793057	12.67792779	$2.77777520 \times 10^{-6}$	$5.55555555 \times 10^{-6}$
190000	12.73199764	12.73199501	$2.63157663 \times 10^{-6}$	$5.26315789 \times 10^{-6}$
200000	12.78329081	12.78328831	$2.49999791 \times 10^{-6}$	$5. \times 10^{-6}$

Observando las dos últimas columnas se puede establecer una mejor estimación del error con $\dfrac{1}{2n}$ y todavía mejor con $\dfrac{1}{2n} - \dfrac{1}{12n^2}$!

n	H_n	$\ln(n) + \gamma + \dfrac{1}{2n} - \dfrac{1}{12n^2}$
100000	12.090146129863427	12.090146129863427
150000	12.495609571309556	12.495609571309554
200000	12.783290810429621	12.783290810429623

También, de estas tablas se puede obtener la aproximación $\gamma \approx 0.577216$

Lema 7.5

$\displaystyle\sum_{k=1}^{n} \tau(k) = nH(n) + O(n)$ y $\displaystyle\sum_{k=1}^{n} \tau(k) \;=\; n\ln(n) + O(n).$

Prueba: Como $\tau(k) = \displaystyle\sum_{d|k} 1$, $\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \sum_{d|k} 1$

La idea ahora es usar argumentos de divisibilidad para usar la expansión del ejemplo 7.3. Si $d|k$ entonces $k = d \cdot c \leq n$. Esto nos dice que el conjunto de todos los divisores positivos de los números k inferiores o iguales a n, se puede describir como el conjunto de todos los pares (c,d) con la propiedad $cd \leq n$ (por supuesto, se puede hacer una demostración formal probando la doble implicación "$\Longleftrightarrow$").

Ahora, $cd \leq n \iff d \leq n \wedge c \leq n/d$. Entonces podemos escribir,

$$\sum_{k=1}^{n} \tau(k) = \sum_{\substack{c,d \\ cd \leq n}} 1 = \sum_{d \leq n} \sum_{c \leq n/d} 1$$

La suma $\displaystyle\sum_{c \leq n/d} 1$ corre sobre los enteros positivos menores o iguales que n/d. Esto nos da $[\![n/d]\!]$ sumandos, i.e. $\displaystyle\sum_{c \leq n/d} 1 = [\![n/d]\!]$. Finalmente, usando el ejemplo 7.3,

$$\begin{aligned}\sum_{k=1}^{n}\tau(k) &= \sum_{d\leq n}[n/d]\\ &= \sum_{d\leq n}\{n/d+O(1)\}\\ &= \sum_{d\leq n}n/d\ +\ \sum_{d\leq n}O(1)\\ &= n\sum_{d\leq n}1/d\ +\ \sum_{d\leq n}O(1)\\ &= n\,H_n+O(n)\end{aligned}$$

En los ejercicios se pide mostrar, usando la figura 7.1, que $H_n=\log(n)+O(1)$. Usando este hecho,

$$\sum_{k=1}^{n}\tau(k)=n\,H_n+O(n)=n\,\{\ln(n)+O(1)\}+O(n)=n\ln(n)+O(n).$$

(Los pequeños detalles que faltan se completan en los ejercicios)

7.7 Acerca de los factores de un número grande

Los siguientes teoremas, los cuales podemos ver en ([8]), nos dan información acerca de qué se podría esperar cuando se intenta factorizar un número grande. Aquí hay que tener cuidado: Las interpretaciones de los teoremas no son del todo rigurosas, solamente son argumentos heurísticos para obtener estimaciones gruesas.

Teorema 7.8

Sea $\pi_k(x)$ el número de enteros $\leq x$ que tienen exactamente k factores primos diferentes, $k\geq 2$. Entonces

$$\pi_k(x)\ \sim\ \frac{6}{\pi^2}\,\frac{x}{\ln x}\,\frac{(\ln\ln x)^{k-1}}{(k-1)!}\ =\ \pi^*(x)\ \ \text{cuando}\ \ x\longrightarrow\infty$$

La aproximación $\pi^*(x)$ de $\pi_k(x)$ funciona si $k=(1+o(1))\ln\ln x$, es decir, si k está en un vecindario de $\ln\ln x$. Por ejemplo, si tomamos $x=10^{100}$ y $k=15$, la proporción de números compuestos (de la totalidad de los compuestos inferiores a x) no da $\approx 0.15\%$. Esto no dice que los números cercanos a $x=10^{100}$, con 15 o más factores, no son muy populares.

Otro teorema útil es el siguiente,

Teorema 7.9

"Normalmente", el número de factores primos diferentes de N es aproximadamente, $\ln\ln N$

En este teorema,"Normalmente" significa que la mayoría de los enteros cercanos a N tienen una cantidad de factores primos entre $(1-\varepsilon)\ln\ln N$ y $(1+\varepsilon)\ln\ln N$ con $\varepsilon>0$.

Ahora, siguiendo un argumento heurístico, podemos concluir que *típicamente*, la cantidad de dígitos del factor primo más grande de N es aproximadamente un 63% de la cantidad de dígitos de N. Si P es el factor primo más grande de N, puesto que $\log N$ es proporcional a la cantidad de dígitos de N, esta estimación se puede poner como $\log P \approx 0.63 \log N$.
La heurística es muy sencilla, si N tiene s factores, N/P tendría $s - 1 \approx \ln\ln N/P = \ln\ln N + \ln(1 - \ln P/\ln N) = s + \ln(1 - \ln P/\ln N)$. Entonces, tomando logaritmo, $1 - \ln P/\ln N \approx 1/e$. Luego, $\ln P \approx (1 - 1/e)\ln N = 0.632 \ln N$.

En particular, para el segundo factor primo P_2 de N, *típicamente* tendríamos $\log P_2 \approx 0.23 \log N$.

Para terminar, vamos a hablar un poco del teorema de Erdös-Kac. El teorema del límite central dice que si una población (continua o discreta) tiene media $\boldsymbol{\mu}$ y varianza finita σ^2, la media muestral $\overline{X}$ tendrá una distribución que se aproxima a la normal.

Teorema 7.10 (Limite Central)

Si tenemos $X_1, X_2, ..., X_n$ variables aleatorias independientes, idénticamente distribuidas, con media $\boldsymbol{\mu}$ y varianza σ^2, entonces, si n es suficientemente grande, la probabilidad de que $S_n = X_1 + X_2 + ... + X_n$ esté entre $n\boldsymbol{\mu} + \alpha\sigma\sqrt{n}$ y $n\boldsymbol{\mu} + \beta\sigma\sqrt{n}$ es

$$\frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\beta} e^{-t^2/2}\, dt$$

Ejemplo 7.17

Si lanzamos una moneda limpia unas 10000 veces, uno esperaría que aproximadamente 5000 veces salga "cara". Si denotamos con $X_i = 1$ el evento "en el lanzamiento i sale cara", como la probabilidad que asumimos para el evento "sale cara" es $1/2$, entonces $n\boldsymbol{\mu} = n \cdot 0.5 = 5000$ y $\sigma = \sqrt{n \cdot 0.25} = 5$. Luego, para calcular la probabilidad de que el número de caras esté entre 4850 y 5150, debemos calcular los límites α y β. Por razones de ajuste del caso discreto al caso continuo, se usa un factor de corrección de $1/2$. Resolviendo, $5000 + (\alpha)\sqrt{50} = 4850 - 0.5 \Longrightarrow \alpha = -3.01$ $5000 + (\alpha)\sqrt{50} = 5150 + 0.5 \Longrightarrow \beta = 3.01$

$$\frac{1}{\sqrt{2\pi}} \int_{-3.01}^{3.01} e^{-t^2/2}\, dt = 0.997388$$

Así, la probabilidad de que el número de caras esté entre 4850 y 5150 es de 0.997388

Si $\omega(n)$ denota la cantidad de factores primos de n, esta función se puede denotar como una suma de funciones $\rho_p(n)$, estadísticamente independientes, definidas por

$$\rho_p(n) = \begin{cases} 1 & \text{si} \quad p|n \\ 0 & \text{si} \quad p \nmid n \end{cases}$$

Esto sugiere que la distribución de los valores de $\omega(n)$ puede ser dada por la ley normal (con media $\ln\ln n$ y desviación estándar $\sqrt{\ln\ln n}$).

Mark Kac y Paul Erdös probaron que la densidad del conjunto de enteros n para el cual el número de divisores primos $\omega(n)$ está comprendido entre $\ln\ln n + \alpha\sqrt{\ln\ln n}$ y $\ln\ln n + \beta\sqrt{\ln\ln n}$, es

$$\frac{1}{\sqrt{2\pi}}\int_\alpha^\beta e^{-t^2/2}\,dt$$

es decir, el número de divisores primos está distribuido de acuerdo a la ley normal.

Teorema 7.11

Denotamos con $N(x,a,b)$ la cantidad de enteros n en $\{3,4,...,x\}$ para los cuales

$$\alpha \leq \frac{\omega(n)-\ln\ln n}{\sqrt{\ln\ln n}} \leq \beta$$

Entonces, conforme $x \to \infty$,

$$N(x,a,b) = (x+o(x))\frac{1}{\sqrt{2\pi}}\int_\alpha^\beta e^{-t^2/2}\,dt$$

EJERCICIOS

7.1 Muestre que $7x^3-12x+9 \ll x^3$ conforme $x\to\infty$. **Ayuda:** Use la derivada.

7.2 Si $f,g:\mathbb{N}\longrightarrow\mathbb{R}^+$, muestre que $\text{Máx}\{f(n),g(n)\} = O(f(n)+g(n))$.

7.3 Muestre que $2^{n+1} = O(2^n)$ pero $2^{2n} \neq O(2^n)$

7.4 Muestre que $f\in O(g)$ no implica necesariamente que $g\in O(f)$

7.5 Si $f(n)\geq 1$ y $\lg[g(n)]\geq 1$ entonces muestre que si $f\in O(g) \implies \lg[f]\in O(\lg[g])$
Ayuda: Use la hipótesis para concluir que $\lg f(n) \leq \lg c + \lg g(n) \leq (\lg c+1)\lg g(n)$.

7.6 Usando la figura 7.1, muestre que $H_n = \log(n)+O(1)$.

7.7 Muestre que $\sum_{d|n}\tau(d)\boldsymbol{\mu}(n/d) = 1$



Parte II

INTRODUCCION A LA TEORIA ALGORITMICA DE NUMEROS.



8 ALGORITMOS PARA EL MCD

"...tal parece que ni siquiera un procedimiento tan venerable como el algoritmo de Euclides puede soportar el progreso"
Donald Knuth ([18], pág 340).

El cálculo del máximo común divisor (mcd) de dos enteros grandes (y también de dos polinomios) es omnipresente en el cálculo con racionales, criptografía de clave pública y álgebra computacional. De hecho los cálculos algebraicos usuales gastan más de la mitad del tiempo de ejecución en el cálculo del máximo común divisor de enteros frecuentemente muy grandes ([16]). Como los cálculos son muy demandantes, se requiere algoritmos muy eficientes para el cálculo del mcd.

Antes de la década de los 70's, el cálculo se hacía con el algoritmo de Euclides clásico o con la versión mejorada de Lehmer[6] (1938). El algoritmo de Euclides (además de su gran valor teórico) es sencillo de enunciar e implementar y es muy eficiente, pero hay algoritmos igual de sencillos y más rápidos. Si los números vienen codificados en binario, teóricamente habría una mejora del 60% ([22]) en la eficiencia. Estos algoritmos se usan desde hace unos cuarenta años atrás. El más popular es el algoritmo "binario" para el cálculo del mcd (algunos autores le llaman "algoritmo binario de Euclides). Este algoritmo fue descubierto por el físico Israelí J. Stein en 1961. D. Knuth hace la observación de que este algoritmo podría tener un pedigrí muy distinguido pues parece ser que ya era conocido en la antigua China (un siglo d.C.). Este último algoritmo solo usa restas, prueba de paridad y divisiones por dos (mucho menos costosas que las divisiones que requiere el algoritmo de Euclides). Desde el punto de vista del computador la división por dos (y también la multiplicación por 2) se hace en representación binaria, así que solo se requiere un desplazamiento de bits. Por ejemplo, $344 = (101011000)_2$, $344/2 = (10101100)_2$ y $2 \cdot 344 = (101011000)_2$. Refiriéndose al algoritmo binario Donald Knuth decía en 1980, "...parece que ni siquiera un procedimiento tan venerable como el algoritmo de Euclides puede soportar el progreso" ([18], pág 340).

Al igual que hay un algoritmo extendido de Euclides también hay una versión extendida del algoritmo binario más eficiente y también hay una versión para polinomios ($\mathbb{Z}[x]$ es tanto un dominio Euclidiano como un "dominio de Stein"). De nuevo aquí, mientras que el algoritmo de

[6] Esta variante del algoritmo de Euclides se aplica para calcular el $\text{mcd}(a,b)$ si a y b son números muy grandes. La idea es aplicar el algoritmo de Euclides usando, en los primeros pasos, $\llbracket a/10^k \rrbracket$ y $\llbracket b/10^k \rrbracket$ en vez de a y b. Una descripción completa se puede ver en [18], págs 345-348.

Euclides requiere, en general, división por polinomios de grado mayor o igual a uno, el algoritmo binario solo requiere dividir por x. Sin embargo, el cálculo del máximo común divisor de dos polinomios con coeficientes enteros no se hace con ninguno de estos algoritmos, más bien se usan algoritmos modulares (Mathematica) o el llamado "algoritmo heurístico para polinomios" (Maple).

El algoritmo de Euclides es muy adecuado para el tratamiento teórico que se hace en los libros de álgebra y teoría de números. Además es muy eficiente para el cálculo. El algoritmo binario y sus variantes (algunas más eficientes que el algoritmo original), aparece de manera natural en el contexto de la teoría algorítmica de números porque aquí si importa ganar en eficiencia. En todo caso, no estaría del todo mal si en los libros de teoría de números, además de incluir notas históricas, apareciera un epílogo contando por donde va la novela en nuestros días.

En este trabajo se muestran cuatro algoritmos: El algoritmo clásico de Euclides, el algoritmo de Euclides con "menor resto", el algoritmo binario y el algoritmo LSBGCD (left-shift binary algorithm) que vendría a ser como una versión binaria del algoritmo de Euclides. Como las implementaciones son sencillas, se implementan en la hoja electrónica de OpenOffice.org, usando el lenguaje OOoBasic.

8.1 Parte entera.

La función parte entera superior de un número x, denotada `ceil(x)`, devuelve el menor entero mayor o igual a x, es decir,

$$\lceil\!\lceil x \rceil\!\rceil = \text{Mín}\{n \in \mathbb{Z} \mid n \geq x\}.$$

Por ejemplo, `Ceil(2.25)=3`, `Ceil(2)=2` y `Ceil(-2.25)=-2`. La función parte entera inferior, denotada `Floor(x)`, devuelve el más grande entero menor o igual a x, es decir,

$$\lfloor\!\lfloor x \rfloor\!\rfloor = \text{Máx}\{n \in \mathbb{Z} \mid n \leq x\}.$$

Por ejemplo, `Floor(2.8)=2`, `Floor(-2)=-2` y `Floor(-2.3)=-3`.

Notemos que $\lceil\!\lceil x \rceil\!\rceil = \lfloor\!\lfloor x \rfloor\!\rfloor$ si y sólo si x es entero, en otro caso $\lceil\!\lceil x \rceil\!\rceil = \lfloor\!\lfloor x \rfloor\!\rfloor + 1$.

El entero "más cercano" a $x \geq 0$ es $\lfloor\!\lfloor x + 1/2 \rfloor\!\rfloor$ ([17],pág 70,ejercicio 5). En la sección 8.4 usaremos la fórmula (para $x \geq 0$),

$$\lfloor\!\lfloor x + 1/2 \rfloor\!\rfloor = \begin{cases} \lfloor\!\lfloor x \rfloor\!\rfloor & \text{si} \quad \text{pfrac}(x) \leq 1/2 \\ \\ \lfloor\!\lfloor x \rfloor\!\rfloor + 1 & \text{si} \quad \text{pfrac}(x) > 1/2 \end{cases} \tag{8.1}$$

donde la parte fraccionaria, denotada "pfrac", de un número real $x \geq 0$ se define con la ecuación

$$x = \lfloor\!\lfloor x \rfloor\!\rfloor + \text{pfrac}(x).$$

Por ejemplo, $2.71 = 2 + 0.71 \Rightarrow \text{pfrac}(x) = 0.71$. En la figura (8.1) se muestra la fórmula desde el punto de vista geométrico.

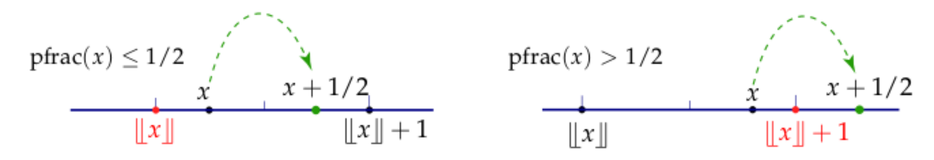


Figura 8.1

Aspectos computacionales. En OOoBasic tenemos la división entera `a\b` (con barra invertida) y la función `Int`.

$$\texttt{Int}(x) = \lfloor x \rfloor \;\; \text{e} \;\; \texttt{Int}(x) + 1 = \lceil x \rceil$$

$$\texttt{a}\backslash\texttt{b} = \begin{cases} \lfloor a/b \rfloor & \text{si} \quad a/b \geq 0 \\ \lceil a/b \rceil & \text{si} \quad a/b < 0 \end{cases}$$

Por ejemplo, `-7`$\backslash$2$= -3$ y `3`$\backslash$2$= 1$.

8.2 División con menor resto.

El teorema de la división[7] establece que si $a, b \in \mathbb{Z}$ con $b \neq 0$, existen $q, r \in \mathbb{Z}$ únicos tales que

$$a = b \cdot q + r \;\; \text{con} \;\; 0 \leq r \leq |b|.$$

A q se le llama *cociente* y r se le llama *resto* y, por supuesto, $r = a - bq$

Esta manera de enunciar este teorema es muy apropiada para fines teóricos. Que el resto sea positivo es adecuado, como vimos, para mostrar unicidad.

Sin embargo el resto no tiene porque ser positivo, por ejemplo si $a = 144$ y $b = 89$,

$$\begin{aligned} 144 &= 89 \cdot 1 + 55, \quad \text{resto} \;\; r_2 = 55 < b = 89 \\ 144 &= 89 \cdot 2 - 34, \quad \text{resto} \;\; r_1 = 34 < b = 89 \end{aligned}$$

Cuando calculamos por ejemplo el máximo común divisor de dos números usando el algoritmo de Euclides, el número de pasos se reduce si tomamos el resto más pequeño en cada paso. Esto no afecta el algoritmo.

[7]Extrañamente a veces a este teorema se le llama "algoritmo de la división". En el contexto computacional, el algoritmo de a división se refiere a los pasos para dividir u por v en el caso de que u y v estén representados en base b. En este caso, el algoritmo calcula $\lfloor u/v \rfloor$.

Veamos los cálculos. Recordemos que $\begin{cases} \operatorname{sgn}(b) = 1 & \text{si} \quad b > 0, \\ \operatorname{sgn}(b) = -1 & \text{si} \quad b < 0. \end{cases}$

Teorema 8.1

Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Sea $q \in \mathbb{Z}$ definido como

$$\begin{cases} q = \lfloor a/b \rfloor & \text{si} \quad b > 0, \\ q = \lfloor a/b \rfloor + 1 & \text{si} \quad b < 0, \ \text{y} \ \ a/b \notin \mathbb{Z} \end{cases} \tag{8.2}$$

entonces la división con resto se puede hacer de dos maneras,

$$\begin{cases} \textbf{a.)} \ a = bq + r_2 & \text{con} \quad 0 \leq r_2 < |b| \\ \textbf{b.)} \ a = b(q + \operatorname{sgn}(b)) - r_1 & \text{con} \quad 0 \leq r_1 < |b| \end{cases}$$

Además, si $a \geq 0$, $b > 0$ y $r = \text{mín}\{r_1, r_2\}$, entonces $r = |a - b \cdot \lfloor a/b + 1/2 \rfloor|$

¿Cómo llegamos a este resultado? Vamos a ver cómo.

Cálculo de q y r_i Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Usando el principio del buen orden se puede establecer que existe $q \in \mathbb{Z}$ tal que bq es el múltiplo de b más cercano a a por la izquierda (ver figura 8.2). Por tanto,

$$bq \leq a < bq + b \ \text{ si } \ b > 0 \qquad \text{y} \qquad bq \leq a < b(q-1) \ \text{ si } \ b < 0.$$

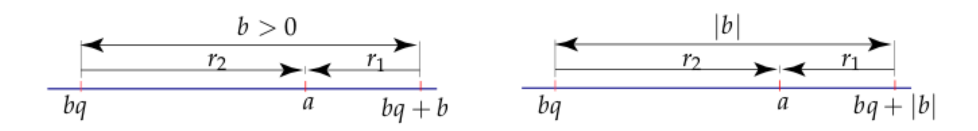


Figura 8.2

Entonces, podemos expresar a en términos de bq con resto positivo o en términos de $bq + |b| = b(q + \operatorname{sng}(b))$ con resto negativo (esta fórmula funciona para b positivo o negativo).

Recordemos que $q = \lfloor a/b \rfloor$ si $b > 0$ y $q = \lceil a/b \rceil$ si $b < 0$. Para usar un mismo q, usamos el hecho de que si $a/b \notin \mathbb{Z}$, entonces $\lceil a/b \rceil = \lfloor a/b \rfloor + 1$ (si $a/b \in Z$ el resto sería cero). Por tanto,

$$\begin{cases} q = \lfloor a/b \rfloor & \text{si} \quad b > 0 \\ q = \lfloor a/b \rfloor + 1 & \text{si} \quad b < 0 \end{cases} \tag{8.3}$$

Entonces tenemos (sin importar el signo de a y b),

$$\begin{cases} \textbf{a.)}\ a = bq + r_2 & \text{con} \quad 0 \leq r_2 < |b| \\ \textbf{b.)}\ a = b(q + \operatorname{sgn}(b)) - r_1 & \text{con} \quad 0 \leq r_1 < |b| \end{cases}$$

Ejemplo 8.1

a.) Si $a = 144$ y $b = 89$,

$$\begin{aligned} 144 &= 89 \cdot 1 + 55, \quad \text{con resto} \ \ r_2 = 55 < b = 89 \\ 144 &= 89 \cdot 2 - 34, \quad \text{con resto} \ \ r_1 = 34 < b = 89 \end{aligned}$$

b.) Si $a = 144$ y $b = -89$, entonces $q = \llbracket 144/(-89) \rrbracket + 1 = -2 + 1 = -1$ y $q + \operatorname{sgn}(b) = -2$. Entonces,

$$\begin{aligned} 144 &= -89 \cdot -1 + 55, \quad \text{con resto} \ \ r_2 = 55 < |b| = 89 \\ 144 &= -89 \cdot -2 - 34, \quad \text{con resto} \ \ r_1 = 34 < |b| = 89 \end{aligned}$$

Cálculo del menor resto. En la sección 8.4 vamos a necesitar el teorema de la división pero con el menor resto. Para simplificar los cálculos, queremos calcular el menor resto usando una fórmula directa. Como se observa en la figura 8.3, uno de los restos es menor que $|b|/2$. Si $r = \text{Mín}\{r_1, r_2\}$ entonces, existe $q' \in \mathbb{Z}$ tal que

$$a = bq' \pm r \quad \text{con} \quad 0 \leq r \leq |b|/2.$$

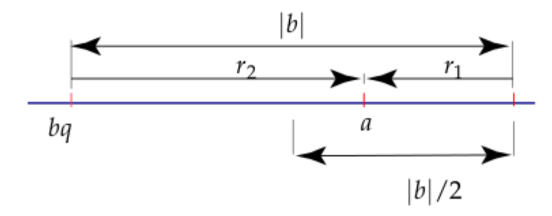


Figura 8.3

Para los cálculos que vamos a hacer aquí solo necesitamos tratar el caso en que $a \geq 0$ y $b > 0$. Para comparar los restos $a - b \cdot \llbracket a/b \rrbracket$ y $b \cdot (\llbracket a/b \rrbracket + 1) - a$ usamos el hecho de que $a/b = \llbracket a/b \rrbracket + \operatorname{pfrac}(a/b)$.

- El menor resto es $a - b \cdot \llbracket a/b \rrbracket$ si $\text{pfrac}(a/b) \leq 1/2$. En efecto,

$$\begin{array}{rcl} a - b \cdot \llbracket a/b \rrbracket & \leq & b \cdot (\llbracket a/b \rrbracket + 1) - a \\ 2a & \leq & 2b \cdot \llbracket a/b \rrbracket + b \\ 2a/b & \leq & 2\llbracket a/b \rrbracket + 1, \quad \text{como} \quad a/b = \llbracket a/b \rrbracket + \text{pfrac}(a/b), \\ \text{pfrac}(a/b) & \leq & 1/2. \end{array}$$

- De manera análoga, $a - b \cdot \llbracket a/b \rrbracket \geq b \cdot (\llbracket a/b \rrbracket + 1) - a$ si $\text{pfrac}(a/b) \geq 1/2$.

Así,

$$\text{el menor resto es } r = \begin{cases} a - b \cdot \llbracket a/b \rrbracket & \text{si} \quad \text{pfrac}(a/b) \leq 1/2, \\ |a - b \cdot (\llbracket a/b \rrbracket + 1)| & \text{si} \quad \text{pfrac}(a/b) > 1/2. \end{cases}$$

Como habíamos establecido antes (ecuación 8.2),

$$\llbracket a/b + 1/2 \rrbracket = \begin{cases} \llbracket a/b \rrbracket & \text{si} \quad \text{pfrac}(a/b) \leq 1/2, \\ \llbracket a/b \rrbracket + 1 & \text{si} \quad \text{pfrac}(a/b) > 1/2, \end{cases}$$

entonces,

$$\text{el menor resto es } r = |a - b \cdot \llbracket a/b + 1/2 \rrbracket|.$$

Aspectos computacionales. En OOoBasic de Libreoffice "el resto" se calcula con la función binaria `Mod`. Se implementa como `a Mod b`$= a - b \cdot ($`a\b`$)$ y tenemos

$$a = b \cdot \texttt{a\\b} + \texttt{a Mod b}$$

Por ejemplo, si $a = -144$ y $b = -89$ entonces `a\b`$= 1$ y `a Mod b`$= -55$.

Si `a Mod b`< 0 y queremos el resto r_2 positivo, la figura 8.3 nos sugiere $r_2 =$ `a Mod b` $+ |b|$, en este caso,

$$a = b \cdot (\texttt{a\\b} - \text{sgn}(b)) + \texttt{a Mod b+|b|}$$

El menor resto se calcula como $r = |a - b \cdot \llbracket a/b + 1/2 \rrbracket|$ =`Abs(a-b*Int(a/b-1/2))`.

8.3 Algoritmo de Euclides II.

El algoritmo de Euclides encuentra el máximo común divisor de dos enteros. Este algoritmo usa divisiones y restas y está basado principalmente en las identidades

$$\text{mcd}\,(a,b) = \text{mcd}\,(b,a-bq),\ \text{mcd}\,(r,0) = r,$$

de tal manera que si $a = bq + r_1$ y $b = r_1q_1 + r_2$ con $0 \leq r_2 < r_1 < b$,

$$\text{mcd}\,(a,b) = \text{mcd}\,(b,r_1) = \text{mcd}\,(r_1,r_2),$$

es decir, conforme aplicamos esta relación, cambiamos el cálculo del mcd de dos números a y b por el mcd de dos números más pequeños. El proceso es finito y se detiene cuando encontramos un resto nulo[8].

Formalmente: Sean a y b números naturales, $b \neq 0$. Aplicando el algoritmo de la división se obtiene una sucesión finita $r_1, r_2, ..., r_n$ definida por

$$\begin{array}{rcll} a & = & bq_1 + r_1, & 0 \leq r_1 < r_0 \\ b & = & r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 & = & r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\ & \vdots & & \\ r_{n-2} & = & r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} & = & r_nq_{n+1} + 0 & \end{array}$$

$r_n = \text{mcd}\,(a,b)$ pues $\text{mcd}\,(a,b) = \text{mcd}\,(b,r_1) = \text{mcd}\,(r_1,r_2) = \ ...\ = \text{mcd}\,(r_n,0) = r_n.$

Ejemplo 8.2

Vamos a aplicar el algoritmo de Euclides para calcular $\text{mcd}\,(89,144)$. Aquí estamos aplicando el algoritmo sobre dos números consecutivos de Fibonacci. Este tipo de pares son los que le demandan mayor esfuerzo al algoritmo de Euclides ([13],págs 68-69) pues siempre $q = 1$.

[8] La versión original de Euclides no es esta, en ese tiempo no había noción del cero ni se consideraba a la unidad como un divisor. Para los griegos antiguos dos enteros positivos eran o ambos iguales a la unidad o eran primos relativos o tenían un máximo común divisor. La versión original ([18],pág 336) sería (sin usar lenguaje geométrico): Sean a,b mayores que la unidad. Si b divide a a, el mcd es b, si el resto de dividir a por b es la unidad, los números son primos relativos, en otro caso reemplace el par de valores (a,b) por (r,b).

$$
\begin{array}{rcllcl}
144 & = & 89\cdot 1+55 & \Longrightarrow \ \text{mcd}\,(89,144) & = & \text{mcd}\,(89,55)\\
89 & = & 55\cdot 1+34 & & = & \text{mcd}\,(55,34)\\
55 & = & 34\cdot 1+21 & & = & \text{mcd}\,(34,21)\\
34 & = & 21\cdot 1+13 & & = & \text{mcd}\,(21,13)\\
21 & = & 13\cdot 1+8 & & = & \text{mcd}\,(13,8)\\
13 & = & 8\cdot 1+5 & & = & \text{mcd}\,(8,5)\\
8 & = & 5\cdot 1+3 & & = & \text{mcd}\,(5,3)\\
5 & = & 3\cdot 1+2 & & = & \text{mcd}\,(3,2)\\
3 & = & 2\cdot 1+1 & & = & \text{mcd}\,(2,1)\\
2 & = & 1\cdot 2+0 & & = & \text{mcd}\,(1,0)=1.
\end{array}
$$

$$\text{mcd}\,(89,144)=1.$$

8.3.1 Algoritmo e implementación.

La implementación de este algoritmo se hace solo con fines ilustrativos. El algoritmo funciona bien si usamos $r =$`a Mod b`. Pero, para seguir el algoritmo al pie de la letra, vamos a usar restos positivos. Se necesitan tres variables: `c` para el nuevo dividendo, d para el nuevo divisor y r para el resto (positivo). La función que calcula q la llamamos `cquo`, es decir, `q=cquo(a,b)`. La función que calcula el resto positivo la llamamos `crem`, `r=crem(a,b)`.

Algoritmo 8.1: Máximo común divisor: Algoritmo de Euclides

Datos: $a,b\in\mathbb{Z},\ b\neq 0$.
Salida: $\text{mcd}\,(a,b)$

```
if a = 0 then
    return mcd(a,b) = |b|
c = |a|, d = |b|;
while d ≠ 0 do
    r = crem(c,d);
    c = d;
    d = r;
return mcd(a,b) = |c|;
```

Ejemplo 8.3

Veamos como funciona el algoritmo, calculamos $\operatorname{mcd}(89,144)$,

$$\begin{array}{rcl}
\overset{\color{red}{c}}{144} & = & \overset{\color{blue}{d}}{89}\cdot 1+\overset{\texttt{crem(c,d)}}{55} \\
 & \swarrow & \\
\overset{\color{red}{c}}{89} & = & \overset{\color{blue}{d}}{55}\cdot 1+\overset{\texttt{crem(c,d)}}{34} \\
 & \swarrow & \\
\overset{\color{red}{c}}{55} & = & \overset{\color{blue}{d}}{34}\cdot 1+\overset{\texttt{crem(c,d)}}{21} \\
 & \swarrow & \\
\overset{\color{red}{c}}{34} & = & \overset{\color{blue}{d}}{21}\cdot 1+\overset{\texttt{crem(c,d)}}{13} \\
 & \swarrow & \\
 & \vdots & \\
\overset{\color{red}{c}}{2} & = & \overset{\color{blue}{d}}{1}\cdot 2+0
\end{array}$$

$\operatorname{mcd}(89,144)=1.$



Implementación en LibreOffice. La función `crem` necesita la función cquo.

[Descargar]

	A	B	C	D	E
1	Algoritmo de Euclides con restos positivos				
2	Máximo común divisor.				Calcular
3	a	b			
4	144	89	144	= 89 * 1 + 55	
5			89	= 55 * 1 + 34	
6			55	= 34 * 1 + 21	
7			34	= 21 * 1 + 13	

```
Function cquo(a,b) As Long
 Dim q As Long
   If b=0 then
      msgbox "Error, b=0"
      Exit Function
   End If
   q = Int(a/b)
   If b<0 Then  q = q+1
   End If
   cquo = q
End Function
```

```
 Function crem(a,b) As Long
      crem = a-b*cquo(a,b) 'rem resto positivo
End Function

 Function mcdEuclides(a,b) As Long
  Dim c As Long, d As Long, r As Long
  If a=0 Then
     c = abs(b)
  Else
    c=a : d=b
    While d<> 0
        r= crem(c,d)
        c = d
        d = r
    Wend
  End If
mcdEuclides = abs(c)
 End Function
```

8.4 Algoritmo de Euclides con menor resto.

En la versión "clásica" del algoritmo de Euclides, el resto r_i está entre 0 y r_{i-1}. Podemos hacer una pequeña variación para que cada nuevos resto r_i esté entre 0 y $r_{i-1}/2$ con lo que, en general, podría haber una reducción en el número de divisiones. Kronecker estableció en 1901 que el número de divisiones en el algoritmo "con menor resto" es menor o igual que el número de divisiones en el algoritmo clásico de Euclides.

Como $\operatorname{mcd}(a,b) = \operatorname{mcd}(|a|,|b|)$ vamos a suponer que $a \geq 0$ y $b > 0$. Recordemos que

$$a = b \cdot \llbracket a/b \rrbracket + r_2. \;\; 0 \leq r_2 < b$$

$$a = b \cdot (\llbracket a/b \rrbracket + 1) - r_1. \;\; 0 \leq r_1 < b$$

Para mejorar un poco el desempeño del algoritmo de Euclides, escogemos en cada paso el menor resto, es decir, $r = \text{Mín}\{r_1, r_2\} = \text{Mín}\{|a - b \cdot \llbracket a/b \rrbracket|,\ |a - b \cdot (\llbracket a/b \rrbracket + 1)|\}$. De esta manera $r \leq b/2$.

El algoritmo de Euclides sigue siendo válido pues si tomamos el menor resto r en cada paso, $\operatorname{mcd}(a,b) = \operatorname{mcd}(b,r)$ y de nuevo obtenemos una sucesión decreciente de restos, el último resto no nulo $|r_n|$ es el mcd de a y b. Por supuesto,

$$r = \text{Mín}\{r_1, r_2\} = a - b \cdot \llbracket a/b + 1/2 \rrbracket.$$

Ejemplo 8.4

Vamos a aplicar el algoritmo de Euclides, usando el menor resto, para calcular $\text{mcd}(89,144)$. Como $\text{mcd}(a,b) = \text{mcd}(|a|,|b|)$, en cada paso usamos dividendo y divisor positivo.

$$\begin{array}{rclcrcl} 144 & = & 89\cdot 2-34 & \Longrightarrow & \text{mcd}(89,144) & = & \text{mcd}(89,34) \\ 89 & = & 34\cdot 3-13 & & & = & \text{mcd}(34,13) \\ 34 & = & 13\cdot 3-5 & & & = & \text{mcd}(13,5) \\ 13 & = & 5\cdot 3+2 & & & = & \text{mcd}(5,2) \\ 5 & = & 2\cdot 2+1 & & & = & \text{mcd}(2,1) \\ 2 & = & 1\cdot 2+0 & & & = & \text{mcd}(1,0)=1 \end{array}$$

$$\text{mcd}(89,144) = 1.$$

8.4.1 Implementación.

La implementación es la misma que la del algoritmo de Euclides clásico. Solo vamos a cambiar la función `crem(a,b)` por la nueva función `srem(a,b)`$= a - b\cdot \lfloor\!\lfloor a/b + 1/2 \rfloor\!\rfloor$. El valor absoluto no es necesario porque lo que interesa en el algoritmo es que los restos disminuyan (en valor absoluto).

```
'-------- LibreOffice Basic
Function mcdMenorResto(a,b) As Long
  Dim c As Long, d As Long, r As Long
  If a=0 Then
     c = b
  Else
    c=a
    d=b
    While d<> 0
        r = c-d*Int(c/d+1/2) 'rem q= Int(c/d+1/2)
        c = d
        d = r
    Wend
  End If
 mcdMenorResto = Abs(c)
 End Function
```

Por ejemplo, si imprimimos cada paso de la implementación con $a = -144$ y $b = -89$, se obtiene

```
-144 = -89*2   + 34      mcd(-144,-89)= mcd(89,34)

-89  =  34*-3  + 13                   = mcd(34,13)

 34  =  13*3   - 5                    = mcd(13,5)

 13  =  -5*-3  - 2                    = mcd(5,2)

-5   =  -2*3   + 1                    = mcd(2,1)

-2   =   1*-2  + 0                    = mcd(1,0)=1
```

8.5 Algoritmo binario.

El algoritmo binario opera con la misma idea, cambiar $\text{mcd}(a,b)$ por el mcd de dos números eventualmente más pequeños, solo que esta vez solo restamos y dividimos por 2. El algoritmo opera con las siguientes teoremas,

Regla 1. Si a,b son pares, $\text{mcd}(a,b) = 2\,\text{mcd}\left(\frac{a}{2},\frac{b}{2}\right)$

Regla 2. Si a es par y b impar, $\text{mcd}(a,b) = \text{mcd}\left(\frac{a}{2},b\right)$

Regla 3. Si a,b son impares, $\text{mcd}(a,b) = \text{mcd}\left(\frac{|a-b|}{2},b\right) = \text{mcd}\left(\frac{|a-b|}{2},a\right)$

La regla 3 se aplica como $\text{mcd}(a,b) = \text{mcd}\left(\frac{|a-b|}{2},\text{Mín}\{a,b\}\right)$. La prueba de estas reglas están al final de esta sección.

El algoritmo procede así: Supongamos que $a,b \in \mathbb{Z}$, $a \geq 0, b > 0$. Si a y b son pares, aplicamos la regla 1, digamos s veces, hasta que alguno de los dos sea impar. Al final hay que multiplicar por 2^s como compensación por haber usado la regla 1, s veces. Si todavía a o b es par, aplicamos la regla 2 hasta que ambos queden impares. Siendo los dos impares, aplicamos la regla 3 y luego alternamos las reglas 2 y 3 conforme el cociente $\frac{|a-b|}{2}$ sea par o impar.

Ejemplo 8.5

Vamos a aplicar el algoritmo de binario para calcular $\text{mcd}(89,144)$ y $\text{mcd}(8,48)$. Recordemos que aquí la ganancia no esta en la disminución del número de pasos (de

hecho podrían ser más pasos que los que utiliza el algoritmo de Euclides) sino en operar dividiendo por 2.

$$\begin{aligned}
\text{mcd}\,(89,44) &= \text{mcd}\,(22,89), && \text{por Regla 2}\\
&= \text{mcd}\,(11,89), && \text{por Regla 2}\\
&= \text{mcd}\,(39,11), && \text{por Regla 3}\\
&= \text{mcd}\,(14,11), && \text{por Regla 3}\\
&= \text{mcd}\,(7,11), && \text{por Regla 2}\\
&= \text{mcd}\,(2,7), && \text{por Regla 3}\\
&= \text{mcd}\,(1,7), && \text{por Regla 2}\\
&= \text{mcd}\,(3,1), && \text{por Regla 2}\\
&= \text{mcd}\,(1,1), && \text{por Regla 3}\\
&= \text{mcd}\,(0,1), && \text{por Regla 3}\\
&= 1
\end{aligned}$$

$$\begin{aligned}
\text{mcd}\,(8,48) &= 2\cdot\text{mcd}\,(4,24), && \text{por Regla 1}\\
&= 4\cdot\text{mcd}\,(2,12), && \text{por Regla 1}\\
&= 8\cdot\text{mcd}\,(1,6) && \text{por Regla 1}\\
&= 8\cdot\text{mcd}\,(1,3), && \text{por Regla 2}\\
&= 8\cdot\text{mcd}\,(1,1), && \text{por Regla 3}\\
&= 8\cdot\text{mcd}\,(0,1), && \text{por Regla 3}\\
&= 8
\end{aligned}$$

Por supuesto, en cálculo manual terminamos cuando obtenemos $\text{mcd}\,(0,d) = d$ o $\text{mcd}\,(1,d) = 1$.

El algoritmo funciona pues la aplicación de las reglas va produciendo una sucesión de pares tal que si (a',b') y (a'',b'') son dos pares consecutivos, entonces $0 \leq a'b' < a''b''$. Este un proceso finito que nos lleva hasta el par $\text{mcd}\,(0,d)$. Para ver esto, observemos que la regla 1 y la regla 2 siempre llevan a la regla 3. Al aplicar esta regla al nuevo par (a,b), si $a = b$ nos queda $\text{mcd}\,(0,\text{mín}\{a,b\})$ y terminamos; sino, supongamos que $0 < a < b$, entonces $\dfrac{b-a}{2} < b/2 < b$, es decir, en esta regla 3 cambiamos a y b por $a' = a$ y $b' = \dfrac{b-a}{2} < b$, por tanto el nuevo par (a',b') cumple $a'b' < ab$. El algoritmo termina cuando obtenemos el par $(0,d)$ y entonces $\text{mcd}\,(a,b) = 2^s \cdot \text{mcd}\,(0,d) = 2^s \cdot d$.

8.5.1 Algoritmo e Implementación.

En la primera parte del algoritmo,si a y $b \neq 0$ son pares, se dividen ambos por dos hasta que uno de los dos sea impar.

Luego, mientras $a \neq 0$, si uno es par y el otro impar, aplicamos la regla dos hasta ambos sean impares. Una vez que los dos son impares, aplicamos la regla tres. Las reglas dos y tres se aplican mientras $a = Abs(a-b)/2$ no se anule.

Aquí suponemos que $a,b \in \mathbb{Z}$, $a \geq 0, b > 0$. La división por 2, denotada $quo(a,2)$ en el algoritmo, se hace con la división entera usual `a\2`.

Algoritmo 8.2: Algoritmo binario para el mcd

```
Datos: a, b ∈ ℤ, a ≥ 0, b > 0
Salida: mcd(a,b)
g = 1;
while rem(a,2) = 0 And rem(b,2) = 0 do
    a = quo(a,2), b = quo(b,2);
    g = 2g //removiendo potencias de 2
while a ≠ 0 do // Ahora, a o b es impar

    if rem(a,2) = 0 then
        a = quo(a,2)
    else if rem(b,2) = 0 then
        b = quo(b,2)
    else ; // ambos impares

        t = quo(|a − b|,2);
        if a ≥ b then ; // reemplazamos máx{a,b} con quo(|a − b|,2)

            a = t
        else
            b = t

return g · b;
```



Implementación en LibreOffice. La implementación es directa. Usamos `a\b` para la división por dos y '`a Mod 2=0`' como prueba de paridad.

[Descargar]

	A	B	C	D
1	Algoritmo binario			
2	Máximo Común Divisor			Calcule
3	a	b	mcd	
4	89	44	1	
5				
6			mcd(89, 22)	
7			mcd(89, 11)	

```
Function mcdBinario(u,v) As Long
 Dim t As Long,  g As Long, a As Long, b As Long
 g=1
 a=Abs(u) : b=Abs(v)
 While a Mod 2=0 And b Mod 2 = 0
       a=a\2
       b=b\2
       g=2*g
 Wend
 While a <> 0
    If       a Mod 2 = 0 Then
             a=a\2
    ElseIf   b Mod 2 =0   Then
             b=b\2
    Else  t=Abs(a-b)/2
          If   a >= b Then
               a=t
          Else b=t
          End If
    End If
 Wend
 mcdBinario=g*b
 End Function
```

Prueba de las reglas. La prueba de las reglas es como sigue.

Prueba de la regla 1. Sean $d = \text{mcd}\,(a,b)$ y $d' = \text{mcd}\left(\frac{a}{2},\frac{b}{2}\right)$. Por el teorema de Bezout, d es la mínima combinación lineal positiva de a y b. Si $d = ax + by > 0$, como a y b son pares, d es par y podemos dividir a ambos lados por 2, $\frac{d}{2} = \frac{a}{2}x + \frac{b}{2} \geq d'$ por ser d' es la mínima combinación lineal positiva de $a/2$ y $b/2$. Por tanto $d \geq 2d'$. De manera análoga se prueba que $2d' \geq d$, con lo cual se concluye $d = 2d'$.

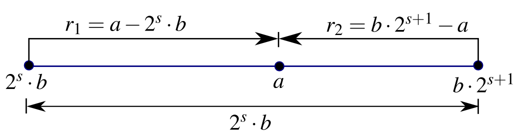
Prueba de la regla 2. Sean $d = \text{mcd}\,(a,b)$ y $d' = \text{mcd}\left(\frac{a}{2},b\right)$. Como $d|b$ y b es impar, d es impar. Si $a = kd$, como a es par y d impar, tenemos que k es par, entonces $\frac{a}{2} = \frac{k}{2}d$, por tanto $d|(a/2)$ y $d|b$, es decir, $d \leq d'$. Ahora como $d'|(a/2)$, $a/2 = k'd'$, es decir $a = 2k'd'$, por tanto $d'|a$, entonces $d'|a$ y $d'|b$, así $d' \leq d$. $\therefore\ d = d'$.

Prueba de la regla 3. Sean $d = \text{mcd}\,(a,b)$ y $d' = \text{mcd}\left(\frac{|a-b|}{2},b\right)$. Como $d|a$ y $d|b$ entonces $d||a-b|$. Como a es impar, d es impar pero $|a-b|$ es par (a y b son impares), luego si $|a-b| = kd$, k debe ser par, así que podemos dividir por dos a ambos lados, $\frac{|a-b|}{2} = \frac{k}{2}d$. Por tanto $d|(|a-b|/2)$ y $d|b$, entonces $d \leq d'$. De manera similar, si $b = k'd'$ y $|a-b| = 2k''d'$, sustituyendo b en la última ecuación obtenemos que $d'|a$. Por tanto $d' \leq d$ y entonces $d = d'$.

8.6 Algoritmo LSBGCD (left-shift binary algorithm)

Este algoritmo debe su nombre al hecho de que se hace multiplicación por 2. En representación binaria el efecto de multiplicar por dos es un desplazamiento (en una posición), de la representación binaria original, hacia la izquierda.

En este algoritmo se encuentra $s \in \mathbb{N}$ tal que $2^s \cdot b \leq a \leq b \cdot (2^{s+1})$ y, como en el algoritmo de Euclides con menor resto, se toma r como el menor resto entre $a - 2^s \cdot b$ y $b \cdot 2^{s+1} - a$.



De esta manera tenemos en el primer paso $a = b \cdot 2^{s'} \pm r \implies \text{mcd}\,(a,b) = \text{mcd}\,(b,r)$; donde s' es s o $s+1$ dependiendo que cual resto sea el menor.

Ejemplo 8.6

Sea $a = 55367$ y $b = 28731$. En cada paso tomamos el menor resto $r = \text{mín}\{a - 2^s \cdot b,\ b \cdot 2^{s+1} - a\}$.

$$\begin{array}{rcll}
55367 &=& 28731 \cdot 2^1 - 2095 \implies \text{mcd}\,(55367,28731) &= \text{mcd}\,(28731,2095)\\
28731 &=& 2095 \cdot 2^4 - 4789 &= \text{mcd}\,(2095,4789)\\
4789 &=& 2095 \cdot 2^1 + 599 &= \text{mcd}\,(2095,599)\\
2095 &=& 599 \cdot 2^2 - 301 &= \text{mcd}\,(599,301)\\
599 &=& 301 \cdot 2^1 - 3 &= \text{mcd}\,(301,3)\\
301 &=& 3 \cdot 2^7 - 83 &= \text{mcd}\,(3,83)\\
83 &=& 3 \cdot 2^5 - 13 &= \text{mcd}\,(3,13)\\
13 &=& 3 \cdot 2^2 + 1 &= \text{mcd}\,(3,1)\\
3 &=& 1 \cdot 2^1 + 1 &= \text{mcd}\,(1,1)\\
1 &=& 1 \cdot 2^0 + 0 &= \text{mcd}\,(1,0) \ = \ 1
\end{array}$$

Como se observa, la sucesión de restos no es una sucesión estrictamente decreciente, pero cada resto r_i está en un intervalo $[0,d_i]$ y el nuevo resto r_{i+1} está en en un intervalo $[0,d_{i+1}] \subset [0,d_i]$, es decir, cada nuevo r_{i+1} está en un intervalo cada vez más pequeño.

Esto es así pues si $a > b$, $a = b \cdot 2^{s_1} + r_1 \implies 0 \leq r_1 < b \cdot 2^{s_1}$. Si $r_1 > 0$. En el siguiente paso tendríamos dos casos posibles,

a.) si $b > r_1$ entonces $b = r_1 \cdot 2^{s_2} + r_2 \implies 0 \leq r_2 < r_1 \cdot 2^{s_2} < b \cdot 2^{s_1}$. Si $r_2 > 0$, la última desigualdad se cumple pues si $r_1 \cdot 2^{s_2} \geq b \cdot 2^{s_1}$ entonces $b = r_1 \cdot 2^{s_2} + r_2 \geq b \cdot 2^{s_1} + r_2$ $(\Rightarrow\Leftarrow)$.

b.) si $r_1 > b$ entonces $r_1 = b \cdot 2^{s_2} + r_2 \implies 0 \leq r_2 < b \cdot 2^{s_2} < b \cdot 2^{s_1}$. Si $r_2 > 0$, la última desigualdad se cumple pues si $b \cdot 2^{s_2} \geq b \cdot 2^{s_1}$ entonces $r_1 = b \cdot 2^{s_2} + r_2 \geq b \cdot 2^{s_1} + r_2$, por tanto $a = b \cdot 2^{s_1} + r_1 \geq b \cdot 2^{s_1} + b \cdot 2^{s_1} + r_2 > b \cdot 2^{s_1+1}$ en contradicción con la escogencia de s_1 (ver figura 8.6).

Si llamamos a los nuevos dividendos $d_1 = b, d_2, d_3$, etc., entonces en el $n-$ésimo resto tendríamos

$$0 \leq r_n < d_n \cdot 2^{s_n} < d_{n-1} \cdot 2^{s_{n-1}} < ... < b \cdot 2^{s_1}$$

Es decir, cada nuevo resto r_i está en un intervalo $[0, d_i \cdot 2^{s_i}]$ cada vez más pequeño. Como el número de intervalos es finito, la sucesión de restos es finita y por tanto en algún momento $r_{n+1} = 0$.

Este algoritmo no es tan rápido como el algoritmo binario, pero su versión extendida si es más eficiente que la versión extendida de Euclides y la versión extendida del algoritmo binario.

8.6.1 Algoritmo e Implementación.

El algoritmo es como sigue,

Algoritmo 8.3: Algoritmo LSBGCD

Datos: $a, b \in \mathbb{Z}^+$ y $a > b$
Salida: mcd(a,b)

```
while b ≠ 0 do
    Calcule s tal que b · 2^s ≤ a < 2^(s+1) b;
    t = Mín{a − b · 2^s, b · 2^(s+1) − a};
    a = b;  b = t;
    if a < b then
        Intercambiar(a,b)
return a
```

Implementación en LibreOffice. Necesitamos una función `Min(a,b)`. Aunque podemos usar la función `Mín` de Calc (vía `createUnoService("com.sun.star.sheet.FunctionAccess")`), aquí no vamos a usar esta posibilidad, más bien usamos una función sencilla.

```
Function Min (a,b) As Long  '------ LibreOffice Basic
Dim m As Long
 m=a
 If a>b Then m=b
 End If
 Min= m
 End Function
```

```
Function LSBMCD(u,v) As Long
 Dim a As Long, b As Long, t As Long, aux As Long
 Dim s As Integer
 a=Abs(u) : b=Abs(v)  rem debe ser a>b

 While b<>0
     s=0
     While b*2^s <=a
        s=s+1
     Wend

     s = s-1 : t=Min(a-b*2^s,b*2^(s+1)-a) : a = b : b = t
     If a<b Then  aux=a  : a=b : b=aux
     End If
 Wend
 LSBMCD = a
End Function
```

8.7 Algoritmo Extendido de Euclides.

Como ya habíamos visto, el máximo común divisor $\operatorname{mcd}(a,b)$ se puede expresar como una combinación lineal de a y b.

Teorema 8.2 (Identidad de Bézout)

Si a,b son dos enteros no ambos cero, existen $s_n, t_n \in \mathbb{Z}$ (no únicos) tales que $s_n a + t_n b = \operatorname{mcd}(a,b)$ donde s_n y t_n se definen recursivamente como

$$\begin{aligned} s_j &= s_{j-2} - q_{j-1}s_{j-1}, \text{ para } j = 2,3,\ldots,n \\ s_0 &= 1, \quad s_1 = 0 \\ t_j &= t_{j-2} - q_{j-1}t_{j-1}, \text{ para } j = 2,3,\ldots,n \\ t_0 &= 1, \quad t_1 = 0 \end{aligned}$$

donde q_{k-1} es el cociente en el $k-$ésimo paso en el algoritmo de Euclides. En particular $r_k = r_{k-2} - r_{k-1}q_{k-1}$ y $r_k = s_k a + t_k b$.

Como se ve, la implemntación a partir del teorema es directa.

8.8 Inversos multiplicativos en $\mathbb{Z}_m$

Si $\operatorname{mcd}(a,m) = 1$ entonces a tiene inverso $x = a^{-1}$, es decir, $ax \equiv 1 \pmod{m}$. Este inverso es único módulo m. Entonces, determinar el inverso de a módulo m es equivalente a resolver la congruencia $ax \equiv 1 \pmod{m}$. Si $\operatorname{mcd}(a,m) = 1$, existen $s,t \in \mathbb{Z}$ tal que $sa + tm = 1$, con lo que

tenemos la solución $x = s$. En la práctica tomamos $a^{-1} = \text{rem}(s, m)$.

Algoritmo 8.4: Inverso Multiplicativo mod m.

Datos: $a \in \mathbb{Z}_m$, $m > 1$
Salida: a^{-1} si $\text{mcd}(a, m) = 1$.

```
Calcular s,t tal que sa + tm = mcd(a,m);
if mcd(a,m) > 1 then
    a^{-1} no existe
else
    return rem(s, m)
```

Java: Para calcular el inverso multiplicativo (si existe) se puede usar el método `modInverse()` de la clase `BigInteger`. Por ejemplo, el código que sigue calcula e imprime en consola el inverso de 5 módulo 7

```
BigInteger b = new BigInteger("5");
System.out.println(b.modInverse(new BigInteger("7")));
```





9 NÚMEROS PRIMOS Y FACTORIZACIÓN.

9.1 Introduccción

En estos capítulos vamos a usar **LibreOffice Basic** para cálculos pequeños y **Java** para cálculos un poco más grandes.

Java. Suponemos que tiene Java instalado en su sistema. En Java, cada algoritmo será un método en la clase `Teoria_Numeros.class`. Las corridas las hacemos en la consola (terminal). Los algoritmos son implementados como métodos públicos y estáticos en esta clase.
Recordemos que los métodos públicos y estáticos los podemos llamar en la clase y desde otras clases (que estén en el mismo folder) sin tener que construir un objeto "`Teoria_Numeros`".
Todos los programa se pueden descargar aquí

Esta clase importa la clase "`BigInteger`". También vamos a implementar y usar una clase `BigRational`. La plantilla de esta clase sería algo como,

```
import java.math.BigInteger;
import java.util.*;
public class Teoria_Numeros
{
  static final BigInteger ZERO=new BigInteger("0");
  static final BigInteger ONE=new BigInteger("1");
  static final BigInteger TWO=new BigInteger("2");
  static final BigInteger THREE=new BigInteger("3");
  static final BigInteger FOUR=new BigInteger("4");

//--------------------- M\'etodos---------------------------------//

//-----------------------------------------------------------------//
 public static void main(String[] args)
 {
      BigInteger a      = new BigInteger("344234534535535424");
      BigInteger b      = new BigInteger("-13444354332434344");
```

```
      BigInteger p,q;
      BigInteger ls[]   = new BigInteger[3];

      System.out.println("\n\n"+ a);
    //--------------------------------------------------------------

    //--------------------------------------------------------------
      System.out.println("\n\n");
  }//fin main
}//fin de la clase
```

Compilar y correr un prorama Java. Para hacer las cosas super sencillas, abrimos un editor de textos (Bloc de Notas en Windows o Gedit en Ubuntu, por ejemplo) y pegamos el código y salvamos el archivo como `Teoria_Numeros.java`. Digamos que guardamos este archivo en la carpeta `'tn/java'`. En **Linux** haríamos las cosas así:

- Abrimos una terminal y vamos a la carpeta que tiene el archivo `Teoria_Numeros.java`, en mi caso, está en el 'Escritorio'. Usamos el comando `cd` para ir a ese directorio,

```
walter-2@walter2-desktop:~$cd /home/walter-2/Escritorio/tn/java   [Enter]
```

- Compilamos con `javac nombre.java`

```
walter-2@walter2-desktop:~/Escritorio/tn/java$ javac Teoria_Numeros.java  [Enter]
```

- "Corremos el programa" con `'java nombre'` (sin extensión). En nuestro caso imprime el 'número grande' a definido en el código.

```
walter-2@walter2-desktop:~/Escritorio/tn/java$ java Teoria_Numeros   [Enter]
```

```
walter-2@walter2-desktop: ~/Escritorio/tn/java
walter-2@walter2-desktop:~$ cd /home/walter-2/Escritorio/tn/java
walter-2@walter2-desktop:~/Escritorio/tn/java$ javac Teoria_Numeros.java
walter-2@walter2-desktop:~/Escritorio/tn/java$ java Teoria_Numeros


34423453453535424


walter-2@walter2-desktop:~/Escritorio/tn/java$
```

Figura 9.1. Compilando y corriendo la la clase `Teoria_Numeros.java`

9.2 Criba de Eratóstenes.

Para efectos de factorización es necesario tener una lista con los “primeros primos” porque ‘casi todos los números’ tiene factores primos pequeños. Esto lo hacemos con la criba de Eratóstenes. Ya habíamos implementado este algoritmo en la sección (2.3). Solo vamos a proceder a la implementación en Java.

Implementación en Java. Vamos a agregar un método a nuestra clase `Teoria_Numeros`. El método recibe el número natural $n > 2$ y devuelve un vector con los números primos $\leq n$. Para colar los números compuestos usamos un arreglo

```
boolean [] esPrimo = new boolean[(n-3)/2].
```

Al final llenamos un vector con los primos que quedan.

```
import java.math.BigInteger;
import java.util.*;
public class Teoria_Numeros
{ static final BigInteger ZERO=new BigInteger("0");
  static final BigInteger ONE=new BigInteger("1");
  static final BigInteger TWO=new BigInteger("2");
  static final BigInteger THREE=new BigInteger("3");
//--------------------- M\'etodos--------------------------------//
public static Vector Primos(int n)
 {          Vector        salida = new Vector(1);
            int k   = 1;
            int max = (n-3)/2;
            boolean[]   esPrimo   = new boolean[max+1];

            for(int i = 0; i <= max; i++)
                esPrimo[i]=true;

            for(int i = 0; (2*i+3) <= n/(2*i+3); i++)
            {
              k = i+1;
              if(esPrimo[i])
              {
                while( 2*k+1<= n/(2*i+3) )
                {
                    esPrimo[((2*k+1)*(2*i+3)-3)/2]=false;
                    k++;
                }
              }
             }
```

```
             salida.addElement(new Integer(2));
             for(int i = 0; i <=max; i++)
             { if(esPrimo[i])
               salida.addElement(new Integer(2*i+3));
             }
             salida.trimToSize();
             return salida;
}//Fin M\'todo Primos

//-----------------------------------------------------------------//
 public static void main(String[] args)
 {
      System.out.println("\n\n");
    //----------------------------------------------------------------
      int    n = 20;
      Vector primos;
             primos = Primos(n);
      //Cantidad de primos <= n
      System.out.println("Primos <="+ n+": "+primos.size()+"\n");
      //Imprimir vector (lista de primos)
      for(int p = 1; p < primos.size(); p++)
      {
          Integer num = (Integer)primos.elementAt(p);
          System.out.println(""+(int)num.intValue());
      }
    //----------------------------------------------------------------
      System.out.println("\n\n");
 }//fin main
}//fin de la clase
```

Una corrida con $n = 20$ nos da la salida en terminal que sigue,

```
walter-2@walter2-desktop:~/Escritorio/tn/java$ javac  Teoria_Numeros.java
Note: Teoria_Numeros2.java uses unchecked or unsafe operations.
Note: Recompile with -Xlint:unchecked for details.
walter-2@walter2-desktop:~/Escritorio/tn/java$ java  Teoria_Numeros

Primos <=20: 8
3
5
7
11
13
17
19
walter-2@walter2-desktop:~/Escritorio/tn/java$
```

Uso de la memoria. En teoría, los arreglos pueden tener tamaño máximo `Integer.MAX_INT` $= 2^{31} - 1 = 2147483647$ (pensemos también en la posibilidad de un arreglo multidimensional!). Pero en la práctica, el máximo tamaño del array depende del hardware de la computadora. El sistema le asigna una cantidad de memoria a cada aplicación; para valores grandes de n puede pasar que se nos agote la memoria (veremos el mensaje "`OutOfMemory Error`"). Podemos asignar una cantidad de memoria apropiada para el programa "cribaEratostenes.java" desde la línea de comandos, si n es muy grande. Por ejemplo, para calcular los primos menores que $n = 100000000$, se puede usar la instrucción

```
walter-2@walter2-desktop:~/Escritorio/tn/java$ java -Xmx1000m -Xms1000m Teoria_Numeros
```

Esta instrucción asigna al programa una memoria inicial (Xmx) de 1000 MB y una memoria máxi-ma (Xms) de 1000 MB (siempre y cuando existan tales recursos de memoria en nuestro sistema).

En todo caso hay que tener en cuenta los siguientes datos

n	Primos $\leq n$
10	4
100	25
1 000	168
10 000	1 229
100 000	9 592
1 000 000	78 498
10 000 000	664 579
100 000 000	5 761 455
1 000 000 000	50 847 534
10 000 000 000	455 052 511
100 000 000 000	4 118 054 813
1 000 000 000 000	37 607 912 018
10 000 000 000 000	346 065 536 839

9.3 Primos entre m y n.

Para encontrar todos los primos entre m y n (con $3 \leq m < n$) procedemos como si estuvieramos colando primos en la lista $\{2, 3, ..., n\}$, solo que esta vez, eliminamos los múltiplos que están entre m y n: Eliminamos los múltiplos de los primos p para los cuales $p^2 \leq n$ (o también $p \leq \sqrt{n}$), que están entre m y n.

Múltiplos de p entre m y n. Para los primos p inferiores a $\sqrt{n}$, buscamos el primer múltiplo de p entre m y n.

Si $m - 1 = pq + r,\ 0 \leq r < p \implies p(q+1) \geq m$

Así, los múltiplos de p mayores o iguales a m son

$$p(q+1),\ p(q+2),\ p(q+3),\ ...\ \text{ con }\ q = \text{quo}(m-1,p)$$

Ejemplo 9.1

Para encontrar los primos entre $m = 10$ y $n = 30$, debemos eliminar los múltiplos de los primos $\leq \sqrt{30} \approx 5$. Es decir, los múltiplos de los primos $p = 2,3,5$.

Como $10 - 1 = 2 \cdot 4 + 1$, el 2 elimina los números $2(4+k) = 8 + 2k$, $k \geq 1$; es decir $\{10,12,...,30\}$

Como $10 - 1 = 3 \cdot 3 + 0$, el 3 elimina los números $3(3+k) = 9 + 3k$, $k \geq 1$; es decir $\{12,15,18,21,24,27,30\}$

Como $10 - 1 = 5 \cdot 1 + 4$, el 5 elimina los números $5(1+k) = 5 + 5k$, $k \geq 1$; es decir $\{10,15,20,25.\}$

Finalmente nos quedan los primos $11,13,17,19,23,29$.

9.3.0.1 Algoritmo e implementación Como antes, solo consideramos los impares entre m y n. Recordemos que si $x \in \mathbb{R}$ y si $n \leq x < n+1$ con $n \in \mathbb{Z}$, entonces la parte entera de x es n. Se escribe $[\![x]\!] = n$.

Sean n,m números naturales tales que $3 \leq m < n$. Sea A el conjunto de números impares entre m y n.

El primer impar de A es $2 \cdot \left[\!\!\left[\frac{m+1-3}{2}\right]\!\!\right] + 3$

El último impar de A es $2 \cdot [\![\frac{n-3}{2}]\!] + 3$

$\therefore$ El conjunto de impares entre m y n es $A = \left\{2 \cdot i + 3 \ :\ i = \left[\!\!\left[\frac{m+1-3}{2}\right]\!\!\right], \cdots, [\![\frac{n-3}{2}]\!]\right\}$.

Si ponemos $min = \text{quo}(m+1-3,2)$ y $max = \text{quo}(n-3,2)$, los impares entre m y n son los elementos del conjunto $\{2 \cdot i + 3 \ :\ i = min,...,max\}$

Como antes, usamos un arreglo booleano `esPrimo(i)` con $i = min,...,max$. `esPrimo(i)` representa al número $2 \cdot i + 3$.

Ejemplo 9.2

Si $m=11$ y 20, $[\![(m+1-3)/2]\!]=4$ y $[\![(n-3)/2]\!]=8$. Luego, el,primer impar es $2\cdot 4+3=11$ y el último impar es $2\cdot 8+3=19$.

Para aplicar el colado necesitamos los primos $\leq \sqrt{n}$. Esta lista de primos la obtenemos con la función `Eratostenes(isqrt(n))`. Aquí hacemos uso del método `BIsqrt(n)`donde n es `BigInteger` (Ver Apéndice **??**). Para cada primo p_i en la lista,

a.) si $m \leq p_i^2$, tachamos los múltiplos impares de p_i como antes,

```
if m ≤ p_i^2 then
    k = (p_i − 1)/2;
    while (2k + 1)p_i ≤ n do
        esPrimo[((2k + 1)p_i − 3)/2] =False;
        k = k + 1;
```

Note que si $k=(p_i-1)/2$ entonces $(2k+1)p_i=p_i^2$

b.) si $p_i^2<m$, tachamos desde el primer múltiplo impar de p_i que supere m :

Los múltiplos de p_i que superan m son $p_i(q+k)$ con $q=\text{quo}(m-1,p)$. De esta lista solo nos interesan los múltiplos impares. Esto requiere un pequeño análisis aritmético.

Como p_i es impar, $p_i(q+k)$ es impar solo si $q+k$ es impar. Poniendo $q_2=\text{rem}(q,2)$ entonces $(2k+1-q_2\ +\ q)$ es impar si $k=q_2,\ q_2+1,\ldots$. En efecto,

$$2k+1-q_2\ +\ q=\begin{cases} 2k+1\ +\ q & \text{si}\quad q\ \text{ es par. Aquí}\quad k=q_2=0,1,\ldots \\ 2k\ +\ q & \text{si}\quad q\ \text{ es impar. Aquí}\quad k=q_2=1,2,\ldots \end{cases}$$

Luego, los múltiplos impares de p_i que superan m son los elementos del conjunto

$$\{(2k+1-q_2\ +\ q)\cdot p_i\ :\ q_2=\text{rem}(q,2)\ \text{ y }\ k=q_2,q_2\ +1,\ldots\}$$

La manera de tachar los múltiplos impares de p_i es

```
if p_i^2 < m then
    q = (m − 1)/p; q_2 = rem(q,2); k = q_2; mp = (2k + 1 − q_2 + q) · p_i ;
    while mp ≤ n do
        esPrimo[(mp − 3)/2] =False;
        k = k + 1;
        mp = (2k + 1 − q_2 + q) · p_i
```

Algoritmo 9.1: Colado de primos entre m y n.

```
Datos: n,m ∈ ℕ con m < n.
Salida: Primos entre m y n
Primo() = una lista de primos ≤ √n;
min = (m + 1 − 3)/2; max = (n − 3)/2;
esPrimo[i], i = min,...,max ;
for j = min,...,max do
    esPrimo[j] =True;
np = cantidad de primos en la lista Primos;
Suponemos Primo(0) = 2;
for i = 1,2,...,np do
    if m ≤ p_i^2 then
        k = (p_i − 1)/2;
        while (2k + 1)p_i ≤ n do
            esPrimo[((2k + 1)p_i − 3)/2] =False;
            k = k + 1;
    if p_i^2 < m then
        q = (m − 1)/p;
        q_2 = rem(q,2);
        k = q_2;
        mp = (2k + 1 − q_2 + q) · p_i ;
        while mp ≤ n do
            esPrimo[(mp − 3)/2] =False;
            k = k + 1;
            mp = (2k + 1 − q_2 + q) · p_i
Imprimir ;
for j = min,...,max do
    if esPrimo[j] =True then
        Imprima 2 · (j + min) + 3
```

Ahora podemos armar el algoritmo completo.

Implementación en Java. Vamos a agregar el método `Primos(m, n)` a nuestra clase "`Teoria_Numeros`". El método recibe dos naturales $0 \leq m < n$ y devuelve un vector con los números primos entre m y n.

Como antes, usamos un arreglo booleano `esPrimo(i)` con $i = 0, ..., max - min + 1$ donde $min = (m+1-3)/2$ y $max = (n-3)/2$.

Si p es primo y $p \leq \sqrt{n}$, entonces si $s \cdot p$ es un múltiplo impar de p entre m y n, debemos poner `esPrimo((s*p-3)/2-min)=false`

Notemos que, `esPrimo(i)` representa al impar $2 \cdot (i + min) + 3$.

```
public class Teoria_Numeros
{
 ...
//-------------------- M\'etodos--------------------------------//
...

public static Vector Primos(int m, int n)
{
    Vector  salida = new Vector(1);
    int k,mip,p,q,q2;
    int min = (m+1-3)/2;
    int max = (n-3)/2;
    int total = max-min+1;
    int sqrtn = BIsqrt(new BigInteger(""+n)).intValue();
    boolean[]   esPrimo   = new boolean[max+1];
    Vector primos;
    primos = Primos(sqrtn);

    if(0<= m && m < 3)
      return Primos(n);

    for(int i = 0; i < total; i++)
        esPrimo[i]=true;
    //primos(0)=2, inicia en primos(1)=3
    for(int i = 1; i< primos.size() ; i++)
    { p =((Integer)primos.elementAt(i)).intValue();
```

```
     if(p*p<m)
     { q=(m-1)/p;
        q2=q%2;
        k=q2;
        mip=(2*k+1-q2+q)*p;
        while(mip<=n)
        {
          esPrimo[(mip-3)/2-min]=false;
          k= k+1;
          mip=(2*k+1-q2+q)*p;
        }
      }
    }
   //Imprimir
  for(int i = 0; i < total; i++)
      if(esPrimo[i])
         salida.addElement(new Integer(2*(i+min)+3));
   salida.trimToSize();
   return salida;
}// Primos n,m

 public static BigInteger BIsqrt(BigInteger n)
{     BigInteger DOS  = new BigInteger("2");
      BigInteger xkm1 = n.divide(DOS);
      BigInteger xk   = n;

      if(n.compareTo(BigInteger.ONE)< 0)
        return xkm1=n;
      while(xkm1.compareTo(xk)<0)
      {
          xk=xkm1;
          xkm1=xkm1.add(n.divide(xkm1));
          xkm1=xkm1.divide(DOS);
      }
      return xkm1;
    }//BIsqrt
//-----------------------------------------------------------------//
 public static void main(String[] args)
 {
      System.out.println("\n\n");
    //-------------------------------------------------------------
      //primos entre m,n
      int m  = 20;
      int n = 50;
      Vector primosmn;
                 primosmn = Primos(m,n);
      for(int j = 0; j < primosmn.size(); j++)
          {       Integer num = (Integer)primosmn.elementAt(j);
                        System.out.println(""+(int)num.intValue());
      }
    //-------------------------------------------------------------
      System.out.println("\n\n");
 }//fin main
}//fin de la clase
```

La corrida, usando $n = 20$ y $m = 50$, entrega el siguiente resultado,

```
walter-2@walter2-desktop:~/Escritorio/tn/java$ javac  Teoria_Numeros.java
walter-2@walter2-desktop:~/Escritorio/tn/java$ java  Teoria_Numeros
23
29
31
37
41
43
47
walter-2@walter2-desktop:~/Escritorio/tn/java$
```

9.4 Factorización por ensayo y error.

El método más sencillo de factorización (y muy útil) es el método de *factorización por ensayo y error* (FEE). Este método va probando con los posibles divisores de n hasta encontrar un factor de este número.

En vez de probar con todos los posibles divisores de n (es decir, en vez de usar *fuerza bruta*) podemos hacer algunos refinamientos para lograr un algoritmo más eficiente en el sentido de reducir las pruebas a un conjunto de números más pequeño, en el que se encuentren los divisores pequeños de n.

9.4.1 Probando con una progresión aritmética.

Como estamos buscando factores pequeños de n, podemos usar el teorema,

Teorema 9.1

Si $n \in \mathbb{Z}^+$ admite la factorización $n = ab$, con $a, b \in \mathbb{Z}^+$ entonces $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.

Del teorema anterior se puede deducir que

- Si n no tiene factores d con $1 < d \leq \sqrt{n}$, entonces n es primo.
- Al menos uno de los factores de n es menor que $\sqrt{n}$ (no necesariamente todos). Por ejemplo $14 = 2 \cdot 7$ solo tiene un factor menor que $\sqrt{14} \approx 3.74166$).

De acuerdo al teorema fundamental de la aritmética, cualquier número natural > 1 factoriza, de manera única (excepto por el orden) como producto de primos. Esto nos dice que la estrategia

óptima de factorización sería probar con los primos menores que $\sqrt{n}$. El problema es que si n es muy grande , el cálculo de los primos de prueba duraría siglos (sin considerar los problemas de almacenar estos números).

Recientemente (2005) se factorizó un número de 200 cifras[9] (RSA-200). Se tardó cerca de 18 meses en completar la factorización con un esfuerzo computacional equivalente a 53 años de trabajo de un CPU 2.2 GHz Opteron.

9.4.2 Algoritmo.

Identificar si un número es primo es generalmente fácil, pero factorizar un número (grande) arbitrario no es sencillo. El método de factorización de un número N probando con divisores primos ("trial division") consiste en probar dividir N con primos pequeños. Para esto se debe previamente almacenar una tabla suficientemente grande de números primos o generar la tabla cada vez. Como ya vimos en la criba de Eratóstenes, esta manera de proceder trae consigo problemas de memoria. En realidad es más ventajoso proceder de otra manera.

- Para hacer la pruebas de divisibilidad usamos los enteros 2, 3 y la sucesión $6k \pm 1$, $k = 1, 2, \ldots$.

  Esta elección cubre todos los primos e incluye divisiones por algunos números compuestos (25,35,...) pero la implementación es sencilla y el programa suficientemente rápido (para números no muy grandes) que vale la pena permitirse estas divisiones inútiles.

- En general, debemos decidir un límite G en la búsqueda de divisores. Si se divide únicamente por divisores primos $\leq G$, se harían $\pi(G) \approx G/\ln G$ divisiones. Si se divide por 2, 3 y $6k \pm 1$ se harían aproximadamente $G/3$ divisiones[10] de las cuales $\dfrac{G/3}{G/\ln G} = 3/\ln G$ son divisiones útiles. Si $G = 10^6$, tendríamos $\approx 22\%$ divisiones útiles. En este caso, un ciclo probando divisiones por primos únicamente es $\approx 1/0.22 = 4.6$ veces más lento[11].

  Cuando se juzga la rapidez de un programa se toma en cuenta el tiempo de corrida en el *peor caso* o se toma en cuenta el *tiempo promedio de corrida* (costo de corrida del programa si se aplica a muchos números). Como ya sabemos (por el Teorema de Mertens) hay un porcentaje muy pequeño de números impares sin divisores $\leq G$, así que en promedio, nuestra implementación terminará bastante antes de alcanzar el límite G (el "peor caso" no es muy frecuente) por lo que tendremos un programa con un comportamiento deseable.

Detalles de la implementación.

[9] Se trata del caso más complicado, un número que factoriza como producto de dos primos (casi) del mismo tamaño.
[10] Pues los números naturales ($\leq G$) son de la forma $6k + m$ con $m \in \{0, 1, ..., 5\}$ y solo estamos considerando $m = 1, 5$, es decir una tercera parte.
[11] Aún si se almacena previamente una tabla de primos en forma compacta, esto consume tiempo [9]

- Para la implementación necesitamos saber cómo generar los enteros de la forma $6k \pm 1$. Alternando el -1 y el 1 obtenemos la sucesión

$$5, 7, 11, 13, 17, 19, ...$$

que iniciando en 5, se obtiene alternando los sumandos 2 y 4. Formalmente, si $m_k = 6k - 1$ y si $s_k = 6k + 1$ entonces, podemos poner la sucesión como

$$7, 11, 13, ..., m_k, s_k, m_{k+1}, s_{k+1}, ...$$

Ahora, notemos que $s_k = m_k + 2$ y que $m_{k+1} = s_k + 4 = m_k + 6$. La sucesión es

$$7, 11, 13, ..., m_k, m_k + 2, m_k + 6, m_{k+1} + 2, m_{k+1} + 6, ...$$

En el programa debemos probar si el número es divisible por 2, por 3 y ejecutamos el ciclo

```
p = 5;
While   p ≤ G Do{
        Probar divisibilidad por p
        Probar divisibilidad por p + 2
        p = p + 6 }
```

- En cada paso debemos verificar si el divisor de prueba `p` alcanzó el límite $\text{Mín}\{G, \sqrt{N}\}$. Si se quiere evitar el cálculo de la raíz, se puede usar el hecho de que si $p > \sqrt{N}$ entonces $p > N/p$.

Algoritmo 9.2: Factorización por Ensayo y Error.

Datos: $N \in \mathbb{N}$, $G \leq \sqrt{N}$
Salida: Un factor $p \leq G$ de N si hubiera.

```
p = 5;
if N es divisible por 2 o 3 then
    Imprimir factor;
else
    while p ≤ G do
        if N es divisible por p o p + 2 then
            Imprimir factor;
            break;
        end
        p = p + 6
    end
end
```

Implementación en Java. El programa que sigue es una clase independiente. Si se quiere, se pueden tomar los métodos y agregarlo a la clase `Teoria_Numeros.java`

Creamos una clase que busca factores primos de un número N hasta un límite G. En el programa, $G =$ Mín $\{\sqrt{N}, G\}$.

Usamos un método `reducir(N,p)` que verifica si p es factor, si es así, continua dividiendo por p hasta que el residuo no sea cero. Retorna la parte de N que no ha sido factorizada.

El método `Factzar_Ensayo_Error(N, G)` llama al método `reducir(N,p)` para cada $p = 2, 3, 7, 11, 13, ...$ hasta que se alcanza el límite G.

```
import java.util.Vector;
import java.math.BigInteger;
public class Ensayo_Error
{   private Vector    salida = new Vector(1);
    static BigInteger Ge     = new BigInteger("10000000");//10^7
    BigInteger        UNO    = new BigInteger("1");
    BigInteger        DOS    = new BigInteger("2");
    BigInteger        TRES   = new BigInteger("3");
    BigInteger        SEIS   = new BigInteger("4");
    BigInteger        Nf;
    int               pos    = 1; //posici\'on del exponente del factor
    public Ensayo_Error(){} //Hay que crear el objeto

    public BigInteger reducir(BigInteger Ne, BigInteger p)
    {   int exp = 0, posAct = pos;
        BigInteger residuo;
        residuo =  Ne.mod(p);
        if(residuo.compareTo(BigInteger.ZERO)==0)
        { salida.addElement(p); //p es objeto BigInteger
          salida.addElement(BigInteger.ONE); //exponente
          pos = pos+2; //posici\'on del siguiente exponente (si hubiera)
        }
        while(residuo.compareTo(BigInteger.ZERO)==0)
        {Ne      =  Ne.divide(p); // Ne = Ne/p
         residuo =  Ne.mod(p);
         exp=exp+1;
         salida.set(posAct, new BigInteger(""+exp)); //p es objeto BigInteger
        }
        return Ne;
     }//
```

```
    public Vector Factzar_Ensayo_Error(BigInteger Ne, BigInteger limG)
    {
        BigInteger p    = new BigInteger("5");
        Nf = Ne;
        Nf = reducir(Nf, DOS);
        Nf = reducir(Nf, TRES);

        while(p.compareTo(limG)<=0)
        {
          Nf= reducir(Nf, p);          //dividir por p
          Nf= reducir(Nf, p.add(DOS)); //dividir por p+2
          p = p.add(SEIS); //p=p+6
        }

        if(Nf.compareTo(BigInteger.ONE)>0)
        {
          salida.addElement(Nf); //p es objeto BigInteger
          salida.addElement(BigInteger.ONE); //exponente
        }
        return salida;
    }
 public static void main(String[] args)
 {
       BigInteger limG;
       BigInteger Nduro    = new BigInteger("2388005888439481");
       BigInteger N        = new BigInteger("27633027771706698949");
       Ensayo_Error Obj    = new Ensayo_Error();
       Vector   factores;

       factores = Obj.Factzar_Ensayo_Error(N); //factoriza

   //Imprimir vector de factores primos
   System.out.println("\n\n");
   System.out.println("N = "+N+"\n\n");
   System.out.println("Hay " +factores.size()/2+" factores primos <= " + Ge+"\n\n");
   System.out.println("N = "+Obj.print(factores)+"\n\n");
   System.out.println("\n\n");
  }
}
```

Al ejecutar este programa en terminal con $N = 367367653565289976655797$, la salida es

```
walter-2@walter2-desktop:~/Escritorio/tn/java$ javac Ensayo_Error.java
walter-2@walter2-desktop:~/Escritorio/tn/java$ java Ensayo_Error

N = 27633027771706698949
```

```
Hay 3 factores primos <= 10000000

N = 37^2 * 3671^3 * 408011^1

walter-2@walter2-desktop:~/Escritorio/tn/java$
```



Implementación en LibreOffice. Se puede hacer una implemetación el LibreOffice, pero por supuesto, como no disponemos de una clase 'BigInteger', solo se pueden factorizar números no más allá de diez dígitos.

[Descargar]

	A	B	C
1	Factorización por Ensayo y Error		
2		Factorice N	
3	N		Factorización
4	35545452		2 · 2 · 3 · 73 · 40577
5			
6			

```
REM  *****  BASIC  *****
Option Explicit
Sub Main
Dim N, G, k
Dim factores As String
Dim factorizacion() As Long
 N =  Celda("A4").Value
 G =  Celda("B4").Value
 G = Sqr(N)
If N < 0 Then
        MsgBox ("Debe introducir un n\'umero natural")
    Else
        factorizacion() = FactorizacionEE(N, G)
        If UBound(factorizacion) = 0 Then
            Celda("C4").setString("")
            Celda("A6").setString("Este n\'umero es primo")
        Else
```

```
            For k = 0 To UBound(factorizacion)
                 If k = 0 Then
                     factores = Trim(str(factorizacion(k)))
                 Else
                    factores = factores +"."+Trim(Str(factorizacion(k)))
                End If
             Next

            Celda("A6").setString(" ")
             Celda("C4").setString(factores)
        End If
    End If
End Sub
Function FactorizacionEE(N, g)
    Dim salir As Boolean
    Dim factor As Long
    Dim factores() As Long
    Dim p As Long, i As Long
    Dim j As Long, prueba
    Dim exp As Long, k
    i = 0
    j = 0
    ReDim factores(i)
    p = 5
    Do
        If N Mod 2 = 0 Then
            factor = 2
            N = N / 2
        ElseIf N Mod 3 = 0 Then
            factor = 3
            N = N / 3
        Else
            While salir = False
                If N Mod p = 0 Then
                    factor = p
                    N = N / p
                    salir = True
                Else
                    p = p + 2
                End If
                If salir = False And N Mod p = 0 Then
                    factor = p
                    N = N / p
                    salir = True
                Else
                    p = p + 4
                End If
                If salir = False And p > g Then
                    salir = True
                    factor = 0
                End If
            Wend
        End If
```

```
        If factor = 0 Then
            ReDim Preserve factores(i)
            factores(i) = N
            i = i + 1
            Exit Do
        Else
            If i - 1 < 0 Then
                ReDim Preserve factores(i)
                factores(i) = factor
                i = i + 1
           Else

                ReDim Preserve factores(i)
                factores(i) = factor
                i = i + 1
            End If
            p = 5
            salir = False
        End If
    Loop Until N = 1
     FactorizacionEE = factores
End Function
```

9.5 Método de factorización "rho" de Pollard.

En el método de factorización por ensayo y error, en su versión más cruda, probamos con todos los números entre 2 y $\sqrt{N}$ para hallar un factor de N. Si no lo hallamos, N es primo. Con el método de factorización "rho" de Pollard podríamos encontrar factores más rápido de tal manera que los factores pequeños que van quedando se pueden factorizar con el método de ensayo y error.

En el método "rho" de Pollard, en vez de hacer estos $\approx \sqrt{N}$ pasos (en el peor caso), vamos a escoger una lista aleatoria de números, más pequeña que $\sqrt{N}$, y probar con ellos.

A menudo se construyen sucesiones *seudo-aleatorias* $x_0, x_1, x_2, ...$ usando una iteración de la forma $x_{i+1} = f(x_i) \,(\text{mod}\, N)$, con $x_0 = \text{random}(0, N-1)$. Entonces $\{x_0, x_1, ...\} \subseteq \mathbb{Z}_N$. Por lo tanto los x_i's se empiezan a repetir en algún momento.

La idea es esta: Supongamos que ya calculamos la sucesión $x_0, x_1, x_2, ...$ y que es "suficientemente aleatoria". Si p es un factor primo de N y si

$$\begin{cases} x_i & \equiv & x_j \,(\text{mod}\, p) \\ x_i & \not\equiv & x_j \,(\text{mod}\, N) \end{cases}$$

entonces, como $x_i - x_j = kp$, resulta que $\text{MCD}(x_i - x_j, N)$ es un factor no trivial de N.

Claro, no conocemos p, pero conocemos los x_i's, así que podemos revelar la existencia de p con el cálculo del MCD: En la práctica se requiere comparar, de manera eficiente, los x_i con los x_j hasta revelar la presencia del factor p vía el cálculo del $\text{MCD}(x_i - x_j, N)$.

$$\begin{cases} x_i & \equiv & x_j \,(\text{mod}\, p) \\ & & \\ x_i & \not\equiv & x_j \,(\text{mod}\, N) \end{cases} \Longrightarrow \text{mcd}\,(x_i - x_j, N) \;\; \text{es factor no trivial de} \;\; N$$

Si $x_0, x_1, x_2, \ldots$ es "suficientemente aleatoria", hay una probabilidad muy alta de que encontremos pronto una "repetición" del tipo $x_i \equiv x_j \,(\text{mod}\, p)$ antes de que esta repetición ocurra (mod N).

Antes de entrar en los detalles del algoritmo y su eficiencia, veamos un ejemplo.

Ejemplo 9.3

Sea $N = 1387$. Para crear una sucesión "seudoaleatoria" usamos $f(x) = x^2 - 1$ y $x_1 = 2$. Luego,

$$\begin{aligned} x_0 &= 2 \\ x_{i+1} &= x_i^2 - 1 \,(\text{mod}\, N) \end{aligned}$$

es decir,

$$\begin{aligned} \{x_0, x_1, x_2, \ldots\} = \; & \{2, 3, 8, 63, 1194, \\ & 1186, 177, 814, 996, 310, 396, 84, 120, 529, 1053, 595, 339, \\ & 1186, 177, 814, 996, 310, 396, 84, 120, 529, 1053, 595, 339, \ldots\} \end{aligned}$$

Luego, "por inspección" logramos ver que $1186 \not\equiv 8 \,(\text{mod}\, N)$ y luego usamos el detector de factores: $\text{mcd}\,(1186 - 8, N) = 19$. Y efectivamente, 19 es un factor de 1387. En este caso detectamos directamente un factor primo de N.

Por supuesto, no se trata de comparar todos los x_i's con los x_j's para $j < i$. El método de factorización "rho" de Pollard, en la variante de R. Brent, usa un algoritmo para detectar rápidamente un ciclo en una sucesión ([28]) y hacer solo unas cuantas comparaciones. Es decir, queremos detectar rápidamente $x_i \equiv x_j \,(\text{mod}\, p)$ usando la sucesión $x_{i+1} = f(x_i) \,(\text{mod}\, N)$ (que alcanza un ciclo un poco más tarde) y el test $\text{mcd}\,(x_i - x_j, N)$.

Típicamente necesitamos unas $O(\sqrt{p})$ operaciones. El argumento es heurístico. Básicamente lo que se muestra es que, como en el problema del cumpleaños, dos números x_i y x_j, tomados de manera aleatoria, son congruentes módulo p con probabilidad mayor que $1/2$, después de que hayan sido seleccionados unos $1.177\sqrt{p}$ números.

Aunque la sucesión $x_{i+1} = f(x_i) \pmod N$ cae en un ciclo en unas $O(\sqrt{N})$ operaciones, es muy probable que detectemos $x_i \equiv x_j \pmod p$ en unos $O(\sqrt{p})$ pasos. Si $p \approx \sqrt{N}$ entonces encontraríamos un factor de N en unos $O(N^{1/4})$ pasos. Esto nos dice que el algoritmo "rho" de Pollard factoriza N^2 con el mismo esfuerzo computacional con el que el método de ensayo y error factoriza N.

9.5.1 Algoritmo e implementación.

La algoritmo original de R. Brent compara x_{2^k-1} con x_j, donde $2^{k+1} - 2^{k-1} \leq j \leq 2^{k+1} - 1$. Los detalles de cómo esta manera de proceder detectan rápidamente un ciclo en una sucesión no se ven aquí pero pueden encontrarse en [28] y [25].

Ejemplo 9.4

Sean $N = 3968039$, $f(x) = x^2 - 1$ y $x_0 = 2$. Luego,

$$\begin{array}{lcl}
\text{mcd}\,(x_1 - x_3, N) & = & 1 \\
\text{mcd}\,(x_3 - x_6, N) & = & 1 \\
\text{mcd}\,(x_3 - x_7, N) & = & 1 \\
\vdots & \vdots & \vdots \\
\text{mcd}\,(x_{63} - x_{96}, N) & = & 1 \\
\text{mcd}\,(x_{63} - x_{97}, N) & = & 1 \\
\text{mcd}\,(x_{63} - x_{98}, N) & = & 1 \\
\text{mcd}\,(x_{63} - x_{99}, N) & = & 1 \\
\text{mcd}\,(x_{63} - x_{100}, N) & = & 1 \\
\text{mcd}\,(x_{63} - x_{101}, N) & = & 1 \\
\text{mcd}\,(x_{63} - x_{102}, N) & = & 1 \\
\text{mcd}\,(x_{63} - x_{103}, N) & = & 1987
\end{array}$$

$N = 1987 \cdot 1997.$

El algoritmo que vamos a describir aquí es otra variante del algoritmo de Brent ([29]) que es más sencillo de implementar.

Después de hacer la implemetación vamos a ver un refinameinto muy sencillo.

Se calcula $\text{MCD}(x_i - x_j, N)$ para $i = 0, 1, 3, 7, 15, \ldots$ y $j = i+1, \ldots, 2i+1$ hasta que, o $x_i = x_j \pmod N$ (en este caso se debe escoger una f diferente o un x_0 diferente) o que un factor no trivial de N sea encontrado.

Observe que si $i = 2^k - 1$ entonces $j = 2i + 1 = 2^{k+1} - 1$, es decir el último j será el 'nuevo' i. Por tanto, en el algoritmo actualizamos x_i al final del `For`, haciendo la asignación $x_i = x_{2i+1} = x_j$.

Algoritmo 9.3: Método rho de Pollard (variante de R. Brent)

Datos: $N \in \mathbb{N}$, f, x_0
Salida: Un factor p de N o mensaje de falla.

salir=false;
$k = 0$, $x_0 =$ Random$(2, N-1)$;
$x_i = x_0$;
while salir=False **do**
    $i = 2^k - 1$;
    for $j = i+1, i+2, ..., 2i+1$ **do**
        $x_j = f(x_0) \pmod N$;
        if $x_i = x_j$ **then**
            salir=True;
            Imprimir "El método falló. Reintentar cambiando f o x_0";
            Exit For;
        $g = \text{mcd}(x_i - x_j, N)$;
        if $1 < g < N$ **then**
            salir=True;
            Imprimir $N = N/g \cdot g$;
            Exit For;
        $x_0 = x_j$;
    $x_i = x_j$;
    $k{+}{+}$;

Implementación en Java. La implementación sigue paso a paso el algoritmo.De nuevo aquí hacemos un programa independiente. Naturalmente, se puede incluir como un conjunto de métodos en `Teoria_Numeros.java`

La corrida de prueba se hace con un número relativamente grande, claro no de varios cientos de dígitos... para eso se necesita otros métodos.

```
import java.math.BigInteger;
public class rhoPollard
{
rhoPollard(){}

public BigInteger f(BigInteger x)
{
    return x.multiply(x).add(BigInteger.ONE);//x^2+1
}

 public  void FactorPollard(BigInteger N)
 {
     int i, k;
     BigInteger xi,xj;
     BigInteger g   = BigInteger.ONE;
     BigInteger x0  = new BigInteger(""+2);;
     boolean salir  = false;

     k = 0;
     xi= x0;
     xj= x0;
     while(salir==false)
     { i=(int)(Math.pow(2,k)-1);
       for(int j=i+1; j<=2*i+1; j++)
       {
           xj=f(x0).mod(N);
           if(xi.compareTo(xj)==0)//si son iguales
           {salir=true;
            System.out.print("Fallo"+"\n\n");
            break;
           }
           g= N.gcd(xi.subtract(xj));
           if(g.compareTo(BigInteger.ONE)==1 && g.compareTo(N)==-1)//1<g<N
           {salir=true;
            System.out.print("Factor = "+g+"\n\n");
            break;
           }
           x0=xj;
       }
       xi=xj;
       k++;
     }
     System.out.print(N+" =  "+g+" . "+N.divide(g)+"\n\n");
  }

  public static void main(String[] args)
  {
   System.out.print("\n\n");
      rhoPollard obj = new rhoPollard();
      BigInteger N = new BigInteger("1000144924286000511176285 9");
      obj.FactorPollard(N);
   System.out.print("\n\n");
 }
}//
```

El resultado de la corrida es,

```
walter-2@walter2-desktop:~/Escritorio/tn/java$ javac rhoPollard.java
walter-2@walter2-desktop:~/Escritorio/tn/java$ java rhoPollard


Factor = 7368787

10001449242860005111762859 =  7368787 . 1357272132151466057



walter-2@walter2-desktop:~/Escritorio/tn/java$
```

Refinamiento. En general, hay muchos casos en los que $\text{MCD}(x_i - x_j, N) = 1$. En vez de calcular todos estos $\text{MCD}(z_1, N)$, $\text{MCD}(z_2, N), \ldots$, calculamos unos pocos $\text{MCD}(Q_k, N)$, donde $Q_k = \prod_{j=1}^{k} z_j \pmod N$. Brent sugiere escoger k entre $\ln N$ y $N^{1/4}$ pero lejos de cualquiera de los dos extremos ([28]). Riesel ([9]) sugiere tomar k como un múltiplo de 100.

Ejemplo 9.5

Sean $N = 3968039$, $f(x) = x^2 - 1$ y $x_0 = 2$. Luego, tomando $k = 30$

$$Q_{30} = \prod_{j=1}^{30} z_j \pmod N = 3105033, \qquad \text{mcd}(Q_{30}, N) = 1$$
$$Q_{60} = \prod_{j=31}^{60} z_j \pmod N = 782878, \qquad \text{mcd}(Q_{60}, N) = 1987$$

EJERCICIOS

9.1 Implementar una variante con el producto $Q_k = \prod_{j=1}^{k} z_j \pmod N$.

9.6 Pruebas de Primalidad.

Para decidir si un número n pequeño es primo, podemos usar el método de ensayo y error para verificar que no tiene divisores primos inferiores a $\sqrt{n}$.

Para un número un poco más grande, la estrategia usual es primero verificar si tiene divisores primos pequeños, sino se usa el test para seudoprimos fuertes de Miller-Rabin con unas pocas bases p_i (con p_i primo) y usualmente se combina con el test de Lucas. Esta manera de proceder decide de manera correcta si un número es primo o no, hasta cierta cota 10^M. Es decir, la combinación de algoritmos decide de manera correcta si $n < 10^M$ Sino, decide de manera correcta

solamente con una alta probabilidad y cabe la (remota) posibilidad de declarar un número compuesto como primo.

Aquí solo vamos a tratar rápidamente la prueba de Miller-Rabin.

9.7 Prueba de primalidad de Miller-Rabin.

Iniciamos con test de primalidad de Fermat, por razones históricas. Esta prueba se basa el el teorema,

Teorema 9.2 (Fermat)

Sea p primo. Si $\text{MCD}(a, p) = 1$ entonces $a^{p-1} \equiv 1 \,(\text{mod}\, p)$.

Este teorema nos dice que si n es primo y a es un entero tal que $1 \leq a \leq n-1$, entonces $a^{n-1} \equiv 1 \,(\text{mod}\, n)$.

Por tanto, n es *compuesto* si encontramos $1 \leq a \leq n-1$ tal que $a^{n-1} \not\equiv 1 \,(\text{mod}\, n)$.

Definición 9.1

Sea n compuesto. Un entero $1 \leq a \leq n-1$ para el que $a^{n-1} \not\equiv 1 \,(\text{mod}\, n)$, se llama "testigo de Fermat" para n.

Un testigo de Fermat para n sería un testigo de no-primalidad. De manera similar, un número $1 \leq a \leq n-1$ para el que $a^{n-1} \equiv 1 \,(\text{mod}\, n)$, apoya la posibilidad de que n sea primo,

Definición 9.2

Sea n un entero compuesto y sea a un entero para el cual $1 \leq a \leq n-1$ y $a^{n-1} \equiv 1 \,(\text{mod}\, n)$. Entonces se dice que n es un seudoprimo respecto a la base a. Al entero a se le llama un "embaucador de Fermat" para n.

Por ejemplo, $n = 645 = 3 \cdot 5 \cdot 43$ es un seudoprimo en base 2 pues $2^{n-1} \equiv 1 \,(\text{mod}\, n)$.

Es curioso que los seudoprimos en base 2 sean muy escasos. Por ejemplo, hay 882206716 primos inferiores a 2×10^{10} y solo hay 19685 seudoprimos en base 2 inferiores a 2×10^{10}. Esto

nos dice que la base 2 parece ser muy poco "embaucadora" en el sentido de que si tomamos un número grande n de manera aleatoria y si verificamos que $2^{n-1} \equiv 1 \,(\bmod\, n)$, entonces es muy probable que n sea primo. También los seudoprimos en base 3 son muy escasos y es altamente improbable que si tomamos un número grande n de manera aleatoria, este sea compuesto y que a la vez sea simultáneamente seudoprimo en base 2 y base 3.

Es decir, si un número n pasa los dos test $2^{n-1} \equiv 1 \,(\bmod\, n)$ y $3^{n-1} \equiv 1 \,(\bmod\, n)$; es muy probable que sea primo.

Sin embargo, hay enteros n compuestos para los cuales $a^{n-1} \equiv 1 \,(\bmod\, n)$ para todo a que cumpla $\text{MCD}(a,n) = 1$. A estos enteros se les llama números de Carmichael.

Por ejemplo, $n = 561 = 3 \cdot 11 \cdot 17$ es número de Carmichael. Aunque este conjunto de números es infinito, son más bien raros (poco densos). En los primeros $100\,000\,000$ números naturales hay 2051 seudoprimos en base 2 y solo 252 números de Carmichael.

Nuestra situación es esta: Es poco probable que un número compuesto pase varios test de "primalidad" $a^{n-1} \equiv 1 \,(\bmod\, n)$ excepto los números de Carmichael, que son compuestos y pasan todos estos test.

Hay otro test, llamado "test fuerte de seudo-primalidad en base a" en el cual los números de Carmichael no pasan. Además, si tomamos k números de manera aleatoria $a_1, a_2, ..., a_k$ y si n pasa este test en cada una de las bases a_i, podemos decir que la probabilidad de que nos equivoquemos al declarar n como primo es menor que $1/4^k$. Por ejemplo, si $k = 200$ la probabilidad de que nos equivoquemos es $< 10^{-120}$

Teorema 9.3

Sea n un primo impar y sea $n - 1 = 2^s r$ con r impar. Sea a un entero tal que $\text{MCD}(a,n) = 1$. Entonces, o $a^r \equiv 1(\bmod\, n)$ o $a^{2^j r} \equiv -1(\bmod\, n)$ para algún j, $0 \leq j \leq s-1$.

Con base en el teorema anterior, tenemos

Definición 9.3

Sea n impar y compuesto y sea $n - 1 = 2^s r$ con r impar. Sea $1 \leq a \leq n-1$.

a.) Si $a^r \not\equiv 1(\bmod\, n)$ y si $a^{2^j r} \not\equiv -1(\bmod\, n)$ para $0 \leq j \leq s-1$, entonces a es llamado un testigo fuerte (de no-primalidad) de n.

b.) Si $a^r \equiv 1(\bmod\, n)$ y si $a^{2^j r} \equiv -1(\bmod\, n)$ para $0 \leq j \leq s-1$, entonces n se dice un seudoprimo fuerte en la base a. Al entero a se le llama "embaucador fuerte".

Así, un seudoprimo fuerte n en base a es un número que actúa como un primo en el sentido del teorema 9.3.

Teorema 9.4 (Rabin)

Si n es un entero compuesto, a lo sumo $\frac{1}{4}$ de todos los números a, $1 \leq a \leq n-1$, son embaucadores fuertes de n.

Supongamos que tenemos un número compuesto n. Tomamos k números $\{a_1, a_2, ..., a_k\}$ de manera aleatoria y aplicamos el test fuerte de seudo-primalidad a n con cada uno de de estas bases a_i. Entonces, hay menos que un chance en cuatro de que a_1 no sea testigo de no-primalidad de n, y menos que un chance en cuatro de que a_2 no sea testigo de no-primalidad de n, etc. Si n es primo, pasa el test para cualquier $a < n$. Si cada a_i falla en probar que n es compuesto, entonces la probabilidad de equivocarnos al decir que n es primo es inferior a $\frac{1}{4^k}$.

9.7.1 Algoritmo e implementación.

Algoritmo 9.4: Miller-Rabin

Datos: $n \geq 3$ y un parámetro de seguridad $t \geq 1$.
Salida: "n es primo" o "n es compuesto".

```
1  Calcule r y s tal que n − 1 = 2^s r, r impar;
2  for i = 1,2,...,t do
3      a = Random(2, n − 2);
4      y = a^r (mod n);
5      if y ≠ 1 y y ≠ n − 1 then
6          j = 1;
7          while j ≤ s − 1 y y ≠ n − 1 do
8              y = y^2 (mod n);
9              if y = 1 then
10                 return "Compuesto";
11             j = j + 1;
12         if y ≠ n − 1 then
13             return "Compuesto";
14 return "Primo";
```

Todo primo impar $n-1$ se puede expresar como $n-1 = 2^j r$, con r impar.

El algoritmo 9.4 verifica si en cada base a se satisface la definición 9.3. En la línea 9, si $y = 1$, entonces $a^{2^j r} \equiv 1 \pmod{n}$. Puesto que este es el caso cuando $a^{2^{j-1} r} \not\equiv \pm 1 \pmod{n}$ entonces n es compuesto. Esto es así pues si $x^2 \equiv y^2 \pmod{n}$ pero si $x \not\equiv \pm y \pmod{n}$, entonces $\text{MCD}(x-y, n)$ es un factor no trivial de n. En la línea 12, si $y \neq n-1$, entonces a es un testigo fuerte de n.

Si el algoritmo 9.4 declara compuesto a n entonces n es definitivamente compuesto, por el teorema 9.3. Si n es primo, es declarado primo. Si n es compuesto, la probabilidad de que el algoritmo lo declare primo es inferior a $1/4^t$.

El algoritmo 9.4 requiere, para $n-1=2^j r$ con r impar, $t(2+j)\ln n$ pasos. t es el número de bases.

Una estrategia que se usa a veces es fijar las bases. Se toman como base algunos de los primeros primos en vez de tomarlas de manera aleatoria. El resultado importante aquí es este: Si $p_1, p_2, ..., p_t$ son los primeros t primos y si ψ_t es el más pequeño entero compuesto el cual es seudoprimo para todas las bases $p_1, p_2, ..., p_t$, entonces el algoritmo de Miller-Rabin, con las bases $p_1, p_2, ..., p_t$, siempre responde de manera correcta si $n < \psi_t$. Para $1 \leq t \leq 8$ tenemos

t	ψ_t
1	2047
2	1 373 653
3	25 326 001
4	3 215 031 751
5	2 152 302 898 747
6	3 474 749 660 383
7	341 550 071 728 321
8	341 550 071 728 321

Implementación en Java. En la clase BigInteger de Java ya viene implementado el método `this.modPow(BigInteger r, BigInteger N)` para calcular $y = a^r \pmod N$. Para calcular r y s solo se divide $N-1$ por dos hasta que el residuo sea diferente de cero.

En esta implementación usamos los primeros ocho primos como bases. Así el algoritmo responde de manera totalmente correcta si $19 < N < 341550071728321$. En todo caso, también podemos usar el método `this.isProbablePrime(int c)` que responde correctamente con una probabilidad que excede $1 - \frac{1}{2^c}$.

```
import java.math.BigInteger;
import java.util.*;
public class Miller_Rabin
{   public Miller_Rabin(){}
    public boolean esPrimoMR(BigInteger N)
    {   //n>3 e impar. Respuesta 100% segura si N <341 550 071 728 321
        BigInteger  N1      = N.subtract(BigInteger.ONE);//N-1
        BigInteger  DOS     = new BigInteger("2");
        int[]       primo   = {2,3,5,7,11,13,17,19};
        int         s       = 0;
        boolean     esPrimo = true;
        BigInteger  a,r,y;
        int         j;
```

```
        while(N1.remainder(DOS).compareTo(BigInteger.ZERO)==0)//n-1 = 2^s r
        {    N1=N1.divide(DOS);
             s=s+1;
        }
        r  = N1;
        N1 = N.subtract(BigInteger.ONE);
        for(int i=0; i<=7; i++)
        {   a = new BigInteger(""+primo[i]);
            y = a.modPow(r, N);
            if( y.compareTo(BigInteger.ONE)!=0 && y.compareTo(N1)!=0)
            { j=1;
               while(j<= s-1 && y.compareTo(N1)!=0 )
               {  y = y.modPow(DOS, N);
                  if(y.compareTo(BigInteger.ONE)==0) esPrimo=false;
                  j++;
               }
               if(y.compareTo(N1)!=0) esPrimo = false;
            }
        }
       return esPrimo;
    }

    public static void main(String[] args)
    {
      System.out.println("\n\n");
      BigInteger  N     = new BigInteger("10011572903");
      Miller_Rabin  obj = new Miller_Rabin();

      System.out.println(N+" es primo = "+obj.esPrimoMR(N)+"\n\n");

      System.out.println("\n\n");
    }
}
```

El resultado de compilar y correr este programa es,

```
walter-2@walter2-desktop:~/Escritorio/tn/java$ javac Miller_Rabin.java
walter-2@walter2-desktop:~/Escritorio/tn/java$ java Miller_Rabin

10011572903 es primo = true

walter-2@walter2-desktop:~/Escritorio/tn/java$
```

EJERCICIOS

9.2 Esta implementación falla para $n = 2,3,5,7,11,13,17,19$. ¿Porqué?

9.3 Mejore la implementación anterior.

9.8 Algoritmo Chino del Resto.

El problema clásico conocido como *problema chino del resto* puede ser establecido como sigue:

Dados los módulos $m_0, m_1, ..., m_k \in \mathbb{Z}$ y los residuos correspondientes $u_i \in \mathbb{Z}_{m_i}$ con $i = 0, 2..., k$; encontrar un entero u tal que

$$u \equiv u_i \pmod{m_i}, \quad 0 \leq i \leq k. \tag{9.1}$$

Las condiciones bajo las cuales se puede garantizar la existencia de una solución única para este problema se establecen en el siguiente teorema,

Teorema 9.5 (Chino del Resto)

Sean $m_0, m_1, ..., m_k \in \mathbb{Z}$ primos relativos dos a dos, i.e. $\operatorname{mcd}(m_i, m_j) = 1$ si $i \neq j$, y consideremos los k residuos $u_i \in \mathbb{Z}_{m_i}, 0 \leq i \leq k$. Para cada entero fijo a existe un único entero $u \in \mathbb{Z}$ que satisface las condiciones

$$\begin{cases} a \leq u < a + m & \text{con } m = \prod_{i=0}^{k} m_i; \\ u \equiv u_i \pmod{m_i}, & 0 \leq i \leq k \end{cases}$$

Ejemplo 9.6

Consideremos $\begin{cases} u \equiv 49 \pmod{99} \\ u \equiv -21 \pmod{97} \\ u \equiv -30 \pmod{95} \end{cases}$

Aquí $m = 912285$. Si $a = 0$ tenemos $u = 639985$.

La unicidad es "módulo m," es decir, el problema chino del resto tiene infinitas soluciones en $\mathbb{Z}$ pero tiene solución única en $\mathbb{Z}_m$, con $m = \prod_{i=0}^{k} m_i$.

Para ver la idea de la prueba, vamos a introducir una notación que nos va a servir más adelante.

Consideremos el *Homomorfismo modular* $\phi_m : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_m[x]$ $(m \geq 2)$, definido por

$$\varphi_m(x) = x$$

$\varphi_m(a) = \text{rem}(a,m)$ para todo $a \in \mathbb{Z}$.

De acuerdo a la definición, $\varphi_m(A(x))$ solo cambia los coeficientes a_i por los nuevos coeficientes $a_i \bmod m$. Por ejemplo, $\varphi_5(3x^6 - x^4 + 6x^3 + x^2 - 3x) = 3x^6 + 4x^4 + x^3 + x^2 + 2x$.

Si $u \in \mathbb{Z}_m$ entonces $(\varphi_{m_0}(u), \varphi_{m_1}(u), ...\varphi_{m_n}(u))$ es uno de los $m = \prod_{i=0}^{n} m_i$ distintos $n+1-$tuples posibles en $\mathbb{Z}_{m_0} \times \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}$. Si calculamos $(\varphi_{m_0}(u), \varphi_{m_1}(u), ...\varphi_{m_n}(u))$ para cada $u \in \mathbb{Z}_m$, en algún momento encontraríamos un $u \in \mathbb{Z}_m$ tal que

$$(\varphi_{m_0}(u), \varphi_{m_1}(u), ...\varphi_{m_n}(u)) = (u_0, u_1, ..., u_n).$$

Así, la unicidad de u debe entenderse en el sentido de que u es único en $\mathbb{Z}_m$ no en $\mathbb{Z}$, es decir u es único módulo m.

La idea de la prueba del teorema chino del resto nos dice cómo encontrar u. Lamentablemente no es práctico buscar u de esta manera pues m puede ser muy grande.

9.8.1 Algoritmo e implementación.

El algoritmo usual para resolver este tipo de problemas se llama "algoritmo de Garner" (por H.L. Garner). La idea central del método de Garner es, a la manera del polinomio interpolante de Newton, *representar* u como una combinación lineal de "base mixta",

$$u = v_0 + v_1\,(m_0) + v_2\,(m_0\,m_1) + ... + v_n\left(\prod_{i=0}^{n-1} m_i\right) \tag{9.2}$$

con $v_k \in \mathbb{Z}_{m_k}$, $k = 0, 1, ..., n$.

Si m es impar, la representación simétrica de $\mathbb{Z}_m$ es $\mathbb{Z}_m = \{-\frac{m-1}{2}, ..., -1, 0, 1, ..., \frac{m-1}{2}\}$

La representación de u como una combinación lineal de "base mixta" tiene sentido si cada $v_k \in \mathbb{Z}_{m_k}$ tiene el mismo tipo de representación, es decir siempre (para cada k) $\mathbb{Z}_{m_k} = \{0, 1, ..., m_k - 1\}$ o siempre $\mathbb{Z}_{m_k} = \{v : -m_k/2 < v \leq m_k/2\}$.

Se puede probar que u siempre se puede representar en la forma (9.2) y, escogida un representación igual para todos los $\mathbb{Z}_{m_k}$, los coeficientes v_i son únicos.

Ejemplo 9.7

Sean $m_0 = 99, m_1 = 97,$ y $m_2 = 95$. Si $u = 639985$,

$$u = 49 + 62 \cdot (m_0) + 66 \cdot (m_0\,m_1).$$

Encontrar u es lo mismo que encontrar $v_0, v_1, ..., v_n$.

Para $i = 0$, de la representación (9.2) se deduce $u \equiv v_0 \pmod{m_0}$. Así que $u \equiv u_0 \pmod{m_0}$ tiene solución $u = u_0$.

Para $k \geq 1$, si se han obtenido los coeficientes $v_0, v_1, ..., v_{k-1}$, entonces de (9.2),

$$u \equiv v_0 + v_1(m_0) + ... + v_k \left(\prod_{i=0}^{k-1} m_i \right) \pmod{m_k}$$

satisface el caso $i = k$ del sistema de congruencias $u \equiv u_i \pmod{m_i}$, $0 \leq i \leq n$, si se toma v_k de tal manera que

$$v_0 + v_1(m_0) + ... + v_k \left(\prod_{i=0}^{k-1} m_i \right) \equiv u_k \pmod{m_k}$$

Esta ecuación la podemos resolver para un único $v_k \in \mathbb{Z}_{m_k}$ $(k \geq 1)$,

$$v_k \equiv \left(u_k - \left[v_0 + v_1(m_0) + ... + v_{k-1} \left(\prod_{i=0}^{k-2} m_i \right) \right] \right) \left(\prod_{i=0}^{k-1} m_i \right)^{-1} \pmod{m_k}$$

El inverso se puede tomar pues $\prod_{i=0}^{k-1} m_i$ y m_k son primos relativos.

Algoritmo 9.5: Problema Chino del Resto en $\mathbb{Z}$. Algoritmo de Garner

Datos: $(u_0, u_1, ... u_n)$, $(m_0, m_1, ..., m_n)$ con $m_i \in \mathbb{Z}$ positivos y primos relativos dos a dos y $u_i \in \mathbb{Z}_{m_i}$.

Salida: $u \in \mathbb{Z}_m$ con $m = \prod_{i=0}^{n} m_i$ tal que $u \equiv u_i \pmod{m_i}$, $i = 0, 1, ..., n$.

```
Cálculo de inversos;
for k = 1 to n do
    producto = φ_{m_k}(m_0);
    for i = 1 to k − 1 do
        producto = φ_{m_k}(producto · m_i);
    γ_k = (producto)^{−1} (mód m_k);
Cálculo de los v_k;
v_0 = u_0;
j = 0;
for k = 1 to n do
    temp = v_{k−1};
    j = k − 2;
    while j ≥ 0 do
        temp = φ_{m_k}(temp · m_j + v_j);
        j = j − 1;
    v_k = φ_{m_k}((u_k − temp)γ_k);
Pasar u a base 10;
u = v_n;
j = n − 1;
while j ≥ 0 do
    u = u · m_j + v_j;
    j = j − 1;
return u;
```

En este algoritmo, la solución u entra "representada" en términos de los $n+1$ residuos $u_0, u_1, ..., u_n$ respecto a los $n+1$ módulos $m_0, m_1, ..., m_n$. Luego se pasa a una representación $v_0, v_1, ..., v_n$ respecto a la base mixta $1, m_0, ..., \prod_{i=0}^{n-1} m_i$ y, como paso final, se reconstruye u en base 10.

Para obtener u en el paso final, se usa una multiplicación anidada

$$u = v_0 + m_0(v_1 + m_1(v_2 + ... + m_{n-2}(v_{n-1} + m_{n-1}(v_n))...))$$

En este último paso, cada iteración actualiza u como $u = u \cdot m_j + v_j$ con $j = n-1, n-2, ..., 0$.

Aquí no es necesario poner $u = \varphi_m(u \cdot m_j + v_j)$ pues estas sumas están en el rango correcto, es decir $u \cdot m_j + v_j \in \mathbb{Z}_m$ no importa la representación que se haya usado. En efecto, como $|v_k| \leq \dfrac{m_k}{2}$ entonces, de acuerdo a (9.2), $|u| \leq (\prod_{i=0}^{n} m_i)/2 = m/2$. Si usamos la representación $\{0, ..., m-1\}$ de $\mathbb{Z}_m$ obtenemos de manera similar, $u \leq m-1$.

Implementación en Java.

```
import java.math.BigInteger;
class PCR
{ PCR(){}
  public BigInteger reprSimetrica(BigInteger m, BigInteger p)
  { BigInteger salida;
    BigInteger DOS = new BigInteger("2");
    salida = m.mod(p);
    //representaci\'on sim\'etrica de Z_p =]-p/2,...-1,0,1,...,p/2]
    //si salida > p/2 -> salida= - p = -p/2 +i.

  if(salida.compareTo(p.divide(DOS))==1)
      salida = salida.add(p.negate());
   return salida;
  }
  //Algoritmo Chino del Resto
  public static BigInteger Z_ACR(BigInteger Uis[], BigInteger Ms[])
  { //Requiere Ms[i]>2.
    int      n      = Ms.length-1; //Ms[0],...,Ms[n]
    BigInteger u    = BigInteger.ZERO;
    BigInteger producto = BigInteger.ONE;
    BigInteger temp;
    BigInteger gamma[] = new BigInteger[n+1]; //gamma[1],...,gamma[n]
    BigInteger v[] = new BigInteger[n+1];
    //para k=1,2,...,n, gamma_k = (Prod mi_{i=0}^{k-1})^{-1} Mod m_k.
    for(int k=1; k<=n; k++)
    {  producto = Ms[0].mod(Ms[k]);
       for(int i=1; i<= k-1; i++)
         producto = (producto.multiply(Ms[i])).mod(Ms[k]);
       gamma[k] = producto.modInverse(Ms[k]);
    }
    int j;
    v[0]=Uis[0];
    for(int k=1; k<=n; k++)
```

```
   {  temp = v[k-1];
      j=k-2;
      while(j>=0)
      {temp = ((temp.multiply(Ms[j])).add(v[j])).mod(Ms[k]);
       j=j-1;
      }
      v[k]= (Uis[k].subtract(temp)).multiply(gamma[k]).mod(Ms[k]);
   }
  u = v[n];
  j = n-1;
  while(j >= 0)
  {u = (u.multiply(Ms[j])).add(v[j]);
   j = j-1;
  }
  return u;
 }
 public static void main(String[] args)
 {
 System.out.print("\n\n");
 PCR     obj = new PCR();

 BigInteger uis[]={new BigInteger("49"),new BigInteger("-21"),
              new BigInteger("-30")};
 BigInteger mis[]={new BigInteger("99"),new BigInteger("97"),
              new BigInteger("95")};

 System.out.println(""+obj.Z_ACR(uis, mis));
 System.out.print("\n\n");
 }
}
```

El programa está preparado para resolver

$$\text{Consideremos}\ \begin{cases} u & \equiv & 49 \pmod{99} \\ u & \equiv & -21 \pmod{97} \\ u & \equiv & -30 \pmod{95} \end{cases}$$

Aquí $m = 912285$. Si $a = 0$ tenemos $u = 639985$. Este resultado se obtuvo después de compilar y correr el programa,

```
walter-2@walter2-desktop:~/Escritorio/tn/java$ javac PCR.java
walter-2@walter2-desktop:~/Escritorio/tn/java$ java PCR

639985

walter-2@walter2-desktop:~/Escritorio/tn/java$
```



Bibliografía

[1] R. Carmichael. *The Theory of Numbers.* 1er Ed. John Wiley and Sons, 1914.

[2] P. Ribenboim. *The Little Book of Bigger Primes.* Springer, 2004.

[3] T. Koshy. *Elementary Number Theory with Applications.* 2da. Ed. Academic Press, 2007.

[4] N. Koblitz *A course in number theory and cryptography.* 2da ed., Springer,1994.

[5] H. Cohen *Number theory. Volume I: Tools and Diophantine Equations.* Springer, 2007.

[6] H. Cohen *A course in computational algebraic number theory.* Springer, 1996.

[7] Lindsay N. Childs. *A Concrete Introduction to Higher Algebra.* Springer-Verlag New York, 1995.

[8] G.H. Hardy, J.E. Littlewood. *An Introduction to Theory of Numbers.* Oxford Univ. Press. 1938.

[9] Hans Riesel. *Prime Numbers and Computer Methods for Factorization.* Springer; 2 edition. 1994.

[10] Mark Kac. *Statistical Independence in Probability Analysis and Number Theory.* John Wiley and Sons, Inc. 1964.

[11] Harold Stark, *An introduction to number theory.* The MIT Press, 1987.

[12] M. Atallah, M. Blanton (2010). *Algorithms and theory of computation handbook. General concepts and techniques.* Chapman & Hall. CRC applied algorithms and data structures series. 2nd ed.

[13] E. Bach, J. Shallit (1996). *Algorithmic Number Theory, Vol. 1: Efficient Algorithms.* Cambridge, MA: MIT Press, 1996.

[14] M. O'Neill., "The Genuine Sieve of Eratosthenes". Journal of Functional Programming. Published online by Cambridge University Press. October 2008.

[15] Jonathan Sorenson. "An Analysis of Two Prime Number Sieves". Computer Sciences Technical Report #1028. Department of Computer Sciences University of Wisconsin-Madison, June 10. 1991

[16] T. Jebelean (1993). "Comparing several GCD algorithms". En ARITH-11: IEEE Symposium on Computer Arithmetic. IEEE, New York, 180-185.

[17] D. Knuth (1981). *The Art of Computer Programming. Volume 1: Fundamental Algorithms.* Addison-Wesley. 2nd ed.

[18] D. Knuth (1981). *The Art of Computer Programming. Volume 2: Seminumerical Algorithms.* Addison-Wesley. 2nd ed.

[19] G. Norton (1987). A shift-remainder GCD algorithm. Proceedings of the 5th international conference, AAECC-5 on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, p.350-356, 1987.

[20] J. Shallit, J. Sorenson (1994). Analysis of a Left-Shift Binary GCD Algorithm. J. Symbolic Computation (1994) 17, 487-511

[21] A. Stepanov (2007). Notes on Programming. En `http://www.stepanovpapers.com`

[22] A. Stepanov, P. McJones (2009). *Elements of Programming.* Addison-Wesley.

[23] A.Weilert (2000). $(1+i)-$ary GCD Computation in $Z[i]$ as an Analogue to the Binary GCD Algorithm.J. Symbolic Computation (2000) 30, 605-617.

[24] William H. Press et all, *NUMERICAL RECIPES. The Art of Scientific Computing.* Third Edition. Cambrifge University Press.

[25] S. Y. Yan. *Number Theory for Computing.* 2nd edition. Springer. 2001.

[26] Eric Weisstein, "Polygonal Number." MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/PolygonalNumber.html

[27] Jim Delany, "Geometric Proof of the Tetrahedral Number Formula". The Wolfram Demonstrations Project. http://demonstrations.wolfram.com/GeometricProofOfTheTetrahedralNumberFormula/

[28] R. Brent. "An Improved Monte Carlo Factorization Algorithm." BIT 20 (1980), 176-184. http://wwwmaths.anu.edu.au/~brent/pub/pubsall.html

[29] R. Brent, J. M. Pollard. "Factorization of the Eighth Fermat Number." Mathematics of Computation, vol 36, n 154 (1981), 627-630. http://wwwmaths.anu.edu.au/~brent/pub/pubsall.html.

[30] Harold M. Edwards. *Riemann's Zeta Function.* Dover Publications Inc. 2001.

Solución de los Ejercicios

Soluciones del Capítulo 2

2.1 $6|2\cdot 3$ pero $6\nmid 2$ y $6\nmid 3$

2.2 si $d|a \,\wedge\, d|(a+1) \implies d|(a+1-a)$ Luego, $d|1 \implies d=\pm 1$.

2.3 Si $kd|n \implies n=k'kd \implies d|n \quad (\Rightarrow\Leftarrow)$

2.4 Como $d|a$ y $d|b \implies d|(a-bq) \implies d|r$

2.5 Como $a-r=bq \quad$ y $\quad 0\leq r<|b|,\ bq$ debe ser uno de los números $\{a,\, a-1,\, ...,a-|b|+1\}$

2.6 $d|a$ y $d|(ab+2) \implies d|ab \,\wedge\, d|(ab+2) \implies d|2 \implies d=1, \vee\, d=2$, pero como a es impar, $d=1$.

2.7 $|A_3\cup B_5\cup C_7|=|A_3|+|B_5|+|C_7|-|A_3\cap B_5|-|B_5\cap C_7|-|C_7\cap A_3|+|A_3\cap B_5\cap C_7|=1629.$

2.9 Si $a=6,\ b=3;\ 3=\operatorname{mcd}(6,3)\neq \operatorname{mcd}(6,6)\neq \operatorname{mcd}(6,6-4\cdot 3)$.

2.10 Sean $d=\operatorname{mcd}(ab,m)$, $d_1=\operatorname{mcd}(a,m)$, $d_2=\operatorname{mcd}(b,m)$. Por Bezout,

$$\left\{\begin{array}{ll} ax_1+my_1 & =d_1 \\ \\ bx_2+my_2 & =d_2 \end{array}\right. \implies abx+my=d_1d_2 \implies d|d_1d_2$$

2.11 Sean $d=\operatorname{mcd}(ab,m)$, $d_1=\operatorname{mcd}(a,m)$, $d_2=\operatorname{mcd}(b,m)$.
Por Bezout, $ax+by=1$, luego $axm+bym=m$. Como d_1 es múltiplo de a y d_2 es múltiplo de m, se sigue $axm=k_1d_1d_2$. De manera análoga, $bym=k_2d_1d_2$.
Así, $d_1d_2|m \wedge d_1d_2|ab$ y entonces $d_1d_2|d$. Usando el ejercicio anterior se concluye que $d_1d_2=d$.

2.13 Por Bezout, existen $x,y,s,t\in\mathbb{Z}$ tal que $\left\{\begin{array}{lcl} ax+by & = & 1 \\ as+ct & = & 1 \end{array}\right.$, Multiplicando obtenemos $a(axs+xct+sby)+bc(yt)=1$, es decir, $\operatorname{mcd}(a,bc)=1$.

2.15 Por Bezout $ax+by=d \implies k_1x+k_2y=1$, por (2.1, 4) $\operatorname{mcd}(k_1,k_2)=1$

2.16 $ra+sb=d \implies rk_1d+sk_2d=d \implies rk_1+sk_2=1 \implies \operatorname{mcd}(r,s)=1$ por (2.1, 4).

2.17 Sea $d=\operatorname{mcd}(a,b)$, a y b son múltiplos de d, entonces $am+bn=h \implies k_1dm+k_2dn=h \implies d|h$.

2.18 "$\implies$": es el ejercicio anterior.
"$\Longleftarrow$": Sea $d=\operatorname{mcd}(a,b)$ y sea $h=kd$. Usando el algoritmo extendido de Euclides podemos calcular $x_1,y_1\in\mathbb{Z}$ tal que $ax_1+by_1=d \implies ax_1k+by_1k=kd=h$. Luego, la solución de la ecuación diofántica es $x=x_1k$ y $y=y_1k$.

2.19 Por el algoritmo extendido de Euclides, $1=365\cdot -699+1876\cdot 136$ luego $24=365\cdot -16776+1876\cdot 3264$

2.20 Sea $\sqrt{k^2-kp}=d\in\mathbb{N}$. Luego $k^2-kp-d^2=0$ de donde

$$k=\frac{p\pm\sqrt{p^2+4\cdot 1\cdot d^2}}{2} \qquad (*)$$

k es entero, así que $\sqrt{p^2+4d^2}$ debe ser cuadrado perfecto, sea $p^2+4d^2=a^2$, entonces $p=(a-2d)(a+2d)$
como p es primo, solo tenemos las dos posibilidades siguientes,

1. $p=(a-2d)$ y $p=(a+2d)$
2. $p^2=a+2d$ y $a-2d=1$ pues $a+2d\geq a-2d$.

En el primer caso $d=0$ (y $a=p$). Entonces $k=0$ o $k=p$
En el segundo caso, resolvemos el sistema y obtenemos $d=(p^2-1)/2$ (y $a=(p^2+1)/2$). Como a,d son naturales, este caso se cumple si p es impar, es decir $p\neq 2$. Sustituyendo d en $(*)$ y resolviendo queda $k=(p+1)/2$ y $k=-(p-1)/2$.

Note que si $p=2$ solo puede suceder el primer caso y queda $k=0$ o $k=2$.

2.21 Para $n=2$ es cierto, por el lema de Euclides.
Si es cierto para $n=k$ y $p_i|(q_1q_2\cdot sq_k)\cdot q_{k+1}$, por el lema de Euclides, $p_i|(q_1q_2\cdot sq_k)$ o $p_i|q_{k+1}$. Aplicando la hipótesis de inducción en el primer caso $p_i|q_j$ para algún $j\in\{1,2,...,k\}$, sino $p_i|q_{k+1}$.

2.26 Sean $a = \prod_i p_i^{\alpha_i}$, $m = \prod_j q_j^{\beta_j}$ y $n = \prod_s r_s^{\delta_s}$ la descomposición prima de estos números. Luego, como mn y a^k son iguales, su descomposición prima es la misma excepto por el orden de los factores, i.e.

$$\prod_j q_j^{\beta_j} \prod_s r_s^{\delta_s} = \prod_i p_i^{k\cdot\alpha_i}$$

Entonces para cada j, $q_j^{\beta_j} = p_{i_j}^{k\cdot\alpha_{i_j}}$ y para cada s, $r_s^{\delta_s} = p_{i_s}^{k\cdot\alpha_{i_s}}$. Luego, $m = \prod_t p_t^{k\alpha_t} = x^k$ y $n = \prod_d p_d^{k\alpha_d} = y^k$.

2.29 Hay un $k \in \mathbb{Z}$ tal que $p-3 = 4k$, entonces $p-7 = 4(k-1)$, por tanto $4|p-7$. Usando la misma idea, comprobamos que $3|p-7$. Como $\operatorname{mcd}(3,4) = 1$, $\operatorname{mcm}(3,4) = 12$ y entonces $12|p-7$.

2.31 Si p_1, p_2, p_3 son primos, $\operatorname{mcd}(p_1p_2,\ p_2p_3,\ p_1,p_3) = 1$ y $\operatorname{mcd}(p_ip_j,\ p_jp_k) \neq 1$. También, si $a = 2\cdot 3\cdot 5$, $b = 5\cdot 7\cdot 11$ y $c = 11\cdot 2$, $\operatorname{mcd}(a,b,c) = 1$
$\operatorname{mcd}(a,b) = 5$
$\operatorname{mcd}(a,c) = 2$
$\operatorname{mcd}(b,c) = 11$

2.32 Sea $d = \operatorname{mcd}(a, a+1)$. Como $d|a \wedge d|(a+1) \implies d|1$. Luego, $d = 1$.
Otra manera: $d = \operatorname{mcd}(a-1, a) \implies d \leq a-(a-1) = 1$ pues d es la mínima combinación lineal positiva de a y $a-1$.

2.33 $m = \operatorname{mcd}(a,b) = \operatorname{mcm}(a,b) \implies m|a \wedge m|b \wedge a|m \wedge b|m \implies a = b$ (por ser ambos positivos).

2.34 Sea $d = \operatorname{mcd}(mg,\ g)$, entonces $d|g \implies d \leq g$. Pero $g|g \wedge g|gm$, entonces $g = d$.

2.35 $\operatorname{mcd}(a,b) = \operatorname{mcd}(a,ka) = a$ según el ejercicio anterior. $\operatorname{mcm}(a,b) = \dfrac{ab}{a} = b$.

2.36 "$\Longrightarrow$": $g|x$ y $g|y \implies g|s$.

"$\Longleftarrow$": $g|s \implies s = kg = (k-1)g + g$. Así, si $x = (k-1)g$ y $y = g$ entonces $s = x+y$ y $\operatorname{mcd}(x,y) = \operatorname{mcd}((k-1)g, g) = g$, por ser g positivo.

2.37 Si $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad+bc}{bd} \in \mathbb{Z}$, entonces $bd|(ad+bc)$. Como $ad+bc = bd$ se tiene que $b|(ad+bc)$ y $d|(ad+bc)$. Luego, $b|ad \wedge d|bc$. Finalmente, como $\operatorname{mcd}(a,b) = \operatorname{mcd}(c,d) = 1$ se concluye que $b|d \wedge d|b$, es decir $|a| = |b|$.

2.38 Sea $d = \operatorname{mcd}(a,\ b)$ y $m = \operatorname{mcd}(a,\ b,\ ax+by)$. Como $d|a \wedge d|b \implies d|(ax+by)$ y por tanto $d|m$.
Luego, como $m|a \wedge m|b \implies m|d$.
$\therefore\ d = m$, por ser ambos positivos.

2.39 $d = \operatorname{mcd}(a, a+2) \implies d|a \wedge d|(a+2) \implies d|2 \implies d = 1 \vee d = 2$.

9.1 Muestre que si $n = pq$, con p,q factores no triviales de n y $p|(y-x)$ y $n \nmid (y-x)$, entonces $1 < \operatorname{mcd}(y-x, n) < n$.

2.40 Usar la factorización prima de N y deducir que sus factores no son los $p_i's$.

2.41 Sea $d_m = \operatorname{mcd}(ma, mb)$ y $d = \operatorname{mcd}(a, b)$. Por Bezout, existen $x, y, s, t \in \mathbb{Z}$ tal que

$d_m = amx + bmy = m(ax + by) = m(kd)$ pues $d|(ax + by)$. Luego, $md|d_m$.

$d = as + bt \implies md = (ma)s + (mb)t \implies d_m|md$.

$md|d_m \wedge d_m|md \implies |d_m| = |md| \implies d_m = |m|d$, por ser d_m y d positivos.

2.42 $d|(2(a + 2b) - (2a + b))$, i.e. $d|3b$.
$d|(2(2a + b) - (a + 2b))$, i.e. $d|3a$
Luego $d|\operatorname{mcd}(3a, 3b) \implies d|3\operatorname{mcd}(a, b) \implies d|3$ por ejercicio(2.41). Luego, $d = 1$ o $d = 3$.

2.43 Asuma que A es entero. Sea 2^α la más grande potencia de 2 que es $\leq n$, i.e. $2^\alpha \leq n$ pero $2^\alpha \cdot 2 > n$.

Considere todas las máximas potencias $p_i^{\beta_i}$, de los *primos impares* p_i, que no exceden n, es decir, $p_i^{\beta_i} \leq n$ pero $p_i^{\beta_i+1} > n$. Sea P es producto de todas estas potencias, $P = \prod_i p_i^{\beta_i}$.

Consideremos el producto

$$2^{\alpha-1}P\left(1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n}\right) = 2^{\alpha-1}P + \frac{2^{\alpha-1}P}{2} + \frac{2^{\alpha-1}P}{3} + ... + \frac{2^{\alpha-1}P}{2^\alpha} + ... + \frac{2^{\alpha-1}P}{n}.$$

Analizamos ahora cada fracción $\dfrac{2^{\alpha-1}P}{k}$. Si k tiene factorización prima $k = 2^\delta \prod_i q_i^{\delta_i}$,

$$\frac{2^{\alpha-1}P}{k} = \begin{cases} \dfrac{2^{\alpha-1}P}{2^\delta \prod_i q_i^{\delta_i}} \\ \\ \dfrac{2^{\alpha-1}P}{2^\alpha} \end{cases}$$

Por definición de P, los q_i aparecen en P pero con una potencia igual o mayor, es decir, para cada i hay un j tal que $q_i = p_j$ y $\delta_i \leq \beta_j$. Luego, como $\delta \leq \alpha - 1$, entonces $\dfrac{2^{\alpha-1}P}{2^\delta \prod_i q_i^{\delta_i}}$ es entero.

Pero, por otra parte, el caso $2^{\alpha-1}P/2^\alpha = P/2 = m + 1/2$ con m entero, por ser P impar. Resumiendo,

$$\begin{aligned} 2^{\alpha-1}PA &= 2^{\alpha-1}P\left(1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n}\right) \\ &= 2^{\alpha-1}P + \frac{2^{\alpha-1}P}{2} + \frac{2^{\alpha-1}P}{3} + ... + \frac{2^{\alpha-1}P}{2^\alpha} + ... \frac{2^{\alpha-1}P}{n} \\ &= Q + P/2 \;=\; Q' + 1/2, \quad \text{con} \quad Q, Q' \quad \text{enteros.} \end{aligned}$$

Pero si A es entero, $2^{\alpha-1}PA$ es entero, mientras que $Q' + 1/2$ no ($\Rightarrow\Leftarrow$).

2.47.a La verificación es directa:

$$\begin{aligned} T_{n-1}^2 - 2T_{n-1} &= (2^{2^{n-1}}+1)^2 - 2(2^{2^{n-1}}+1) \\ &= 2^{2^{n-1}\cdot 2} + 2\cdot 2^{2^{n-1}} + 1 - 2\cdot 2^{2^{n-1}} - 2 \\ &= 2^{2^n} - 1 \end{aligned}$$

2.47.b La fórmula anterior es una fórmula recursiva:

$2^{2^n} - 1 = T_n - 2 = T_{n-1}^2 - 2T_{n-1} = T_{n-1}(T_{n-1}-2)$, i.e.
$T_n - 2 = T_{n-1}(T_{n-1}-2)$. Luego,

$$\begin{aligned} T_n - 2 &= T_{n-1}(T_{n-1}-2) \\ &= T_{n-1}(T_{n-2}(T_{n-2}-2)) \\ &= T_{n-1}T_{n-2}T_{n-3}(T_{n-3}-2) \\ &\vdots \\ &= T_{n-1}T_{n-2}T_{n-3}\cdot sT_0(T_0-2) \\ &= T_{n-1}T_{n-2}T_{n-3}\cdot sT_0, \quad \text{pues} \quad T_0 - 2 = 3 - 2 = 1 \end{aligned}$$

2.47.c $T_m = T_{m-1}\cdot sT_n \cdot sT_0 + 2$. Si $\text{mcd}\,(T_n, T_m) = d$ entonces $d|T_m \implies d|(T_{m-1}\cdot sT_n\cdot sT_0 + 2)$ y como $d|T_n$, $d|2$. Así que $d = 1$ o $d = 2$. Pero por definición, T_m y T_n son impares.